NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Comments on Cyber Security Ninety-day Response — Project 2009-21

The Cyber Security Order 706 Standard Drafting Team thanks all commenters who submitted comments on the proposed revisions of CIP-002-2 through CIP-009-2, the Implementation Plan for Version 3 of the Cyber Security Standards, and the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities, developed by the standard drafting team as part of Project 2009-21 Cyber Security Ninety-day Response. These standards were posted for a 30-day public comment period from October 13, 2009 through November 12, 2009. The respondents were asked to provide feedback on the standards through a special Electronic Comment Form. There were 29 sets of comments, including comments from more than 60 different people from approximately 40 companies representing 8 of the 10 Industry Segments as shown in the table on the following pages.

http://www.nerc.com/filez/standards/Project2009-21_Cyber_Security_90-day_Response.html

The drafting team made the following changes following the initial comment period, prior to the initial ballot:

Changes to CIP-006-3

- In response to stakeholder comments the drafting team revised CIP-006-3 Requirement R1.6 as shown below to more closely address the specific directive included in the FERC Order approving Version 2 CIP Standards issued September 30, 2009.

  R1.6. A visitor control program for visitors (personnel without authorized unescorted access to a Physical Security Perimeter), containing at a minimum the following:
  R1.6.1. Logs (manual or automated) to document the entry and exit of visitors, including the date and time, to and from Physical Security Perimeters.
  R1.6.2. Continuous escorted access of visitors within the Physical Security Perimeter.

Changes to Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities

- Several stakeholders also asked for clarity on the following language that had been in the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities concerning the date of first occurrence of a recurring requirement:

  > A number of the NERC Reliability Standard requirements include a prescribed periodicity or recurrence of the requirement activity (e.g., an annual review of documentation). In those instances, the first occurrence of the recurring requirement must be completed by the Compliant milestone date in Table 2. The entity is then required to collect and maintain required "data," "documents," "documentation," "logs," and "records" to demonstrate compliance with the recurring requirement after the Compliant milestone date has been reached.
  >
  > For those NERC Reliability Standard requirements that include a prescribed records retention period (e.g., retention of logs for 90 days), a Responsible Entity is expected to begin collection and retention of the required "data," "documents," "documentation," "logs," and "records" by the Compliant milestone date in Table 2.

For retention requirements that are triggered by a specific event (e.g., a reportable incident), collection and retention of the required "data," "documents," "documentation," "logs," and "records" begins with the triggering event. In this instance, the requirement for records collection and retention does not begin until the Compliant milestone date in Table 2 is reached and only applies to triggering events occurring after the Compliant milestone date.

The SDT acknowledged that the initial performance date of tasks being performed as part of meeting recurring requirements is problematic from an audit perspective. The SDT also acknowledged that this issue is not confined to the CIP standards alone and hence goes beyond the scope of this SDT. The drafting team removed the language from the implementation plan. The NERC Compliance Staff is expected to issue a compliance bulletin addressing this issue.

- The team also added language to clarify the meaning of the terms "compliant" and "auditably compliant" as used in the implementation plan, and added some language to clarify when to apply the "Category 1 Scenario" and "Category 2 Scenario" referenced in the plan, and changed some headings for improved clarity.

Changes to Implementation Plan for Version 3 of Cyber Security Standards CIP-002-3 through CIP-009-3

- The drafting team modified the section of the plan that addressed retirement of earlier implementation plans to improve clarity.

The drafting team did not make any changes to the SAR, or to the proposed VRFs or VSLs that were posted for comment.

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.

Index to Questions, Comments, and Responses

The Industry Segments are:

1 — Transmission Owners
2 — RTOs, ISOs
3 — Load-serving Entities
4 — Transmission-dependent Utilities
5 — Electric Generators
6 — Electricity Brokers, Aggregators, and Marketers
7 — Large Electricity End Users
8 — Small Electricity End Users
9 — Federal, State, Provincial Regulatory or other Government Entities
10 — Regional Reliability Organizations, Regional Entities

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
1.	Group	Guy Zito	Northeast Power Coordinating Council										X

	Additional Member	Additional Organization	Region	Segment Selection
1.	Ralph Rufrano	New York Power Authority	NPCC	5
2.	Alan Adamson	New York State Reliability Council, LLC	NPCC	10
3.	Gregory Campoli	New York Independent System Operator	NPCC	2
4.	Roger Champagne	Hydro-Quebec TransEnergie	NPCC	2
5.	Kurtis Chong	Independent Electricity System Operator	NPCC	2
6.	Sylvain Clermont	Hydro-Quebec TransEnergie	NPCC	1
7.	Chris de Graffenried	Consolidated Edison Co. of New York, Inc.	NPCC	1
8.	Brian D. Evans-Mongeon	Utility Services	NPCC	8
9.	Mike Garton	Dominion Resouces Services, Inc.	NPCC	5
10.	Brian L. Gooder	Ontario Power Generation Incorporated	NPCC	5
11.	Kathleen Goodman	ISO - New England	NPCC	2
12.	David Kiguel	Hydro One Networks Inc.	NPCC	1
13.	Michael R. Lombardi	Northeast Utilities	NPCC	1
14.	Randy MacDonald	New Brunswick System Operator	NPCC	2

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
15.	Greg Mason		Dynegy Generation	NPCC						5			
16.	Bruce Metruck		New York Power Authority	NPCC						6			
17.	Chris Orzel		FPL Energy/NextEra Energy	NPCC						5			
18.	Robert Pellegrini		The United Illuminating Company	NPCC						1			
19.	Saurabh Saksena		National Grid	NPCC						1			
20.	Michael Schiavone		National Grid	NPCC						1			
21.	Peter Yost		Consolidated Edison Co. of New York, Inc.	NPCC						3			
22.	Gerry Dunbar		Northeast Power Coordinating Council	NPCC						10			
23.	Lee Pedowicz		Northeast Power Coordinating Council	NPCC						10			
2.	Group	Ruth Blevins	Dominion Virginia Power	X		X		X					
	Additional Member		**Additional Organization**	**Region**						**Segment Selection**			
1.	john calder			SERC						1, 3			
2.	dennis sollars			SERC						1, 3, 5			
3.	paul rodi			SERC						5			
4.	randy reynolds			SERC						1			
5.	george wood			SERC						1			
3.	Group	Sam Ciccone	FirstEnergy	X		X	X	X	X				
	Additional Member		**Additional Organization**	**Region**						**Segment Selection**			
1.	Doug Hohlbaugh		FirstEnergy	RFC						1, 3, 4, 5, 6			
2.	Dave Folk		FirstEnergy	RFC						1, 3, 4, 5, 6			
4.	Group	Denise Koehn	Bonneville Power Administration	X		X		X	X				
	Additional Member		**Additional Organization**	**Region**						**Segment Selection**			
1.	Curt Wilkins		Transmission System Operations	WECC						1			
2.	Kelly Hazelton		Transmission System Operations	WECC						1			
5.	Group	Jason L. Marshall	Midwest ISO Standards Collaborators		X								

	Commenter	Organization	Industry Segment									
			1	2	3	4	5	6	7	8	9	10
	Additional Member	**Additional Organization**	**Region**						**Segment Selection**			
1.	Barb Kedrowski	We Energies	RFC						3, 4, 5			
2.	Michael Ayotte	ITC Holdings	RFC						1			
3.	Greg Rowland	Duke Energy	SERC						1, 3, 5, 6			
4.	Joe Knight	GRE	MRO						1, 3, 5			
5.	Eric Scott	Ameren	SERC						1			
6.	Bob Thomas	IMEA	SERC						4			
6.	Individual	Laurie Urbancik	Exelon									
7.	Individual	Sandra Shaffer	PacifiCorp	X		X		X	X				
8.	Individual	Ed Carmen	BGE CIP Core Team	X									
9.	Individual	Silvia Parada-Mitchell	Transmission Owner	X				X	X				
10.	Individual	Brent Ingebrigtson	E.ON U.S. LLC	X		X		X	X				
11.	Individual	Benjamin Church	NextEra Energy Resources					X					
12.	Individual	Jim Lauth	Silicon Valley Power			X	X	X					
13.	Individual	Jeremy Bergstrom	Navasota Odessa Energy Partners, LP					X					
14.	Individual	Kasia Mihalchuk	Manitoba Hydro	X		X		X	X				
15.	Individual	Michael Puscas	The United Illuminating Company	X		X							
16.	Individual	James Starling	South Carolina Electric and Gas	X		X		X	X				
17.	Individual	Steve Newman	MidAmerican Energy Company	X		X		X	X				

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
18.	Individual	Marty Berland	Progress Energy	X		X		X	X				
19.	Individual	Randy Schimka	San Diego Gas and Electric Co	X		X		X					
20.	Individual	James H. Sorrels, Jr.	American Electric Power	X		X		X	X				
21.	Individual	Patrick Brown	PJM Interconnection		X								
22.	Individual	Adam Menendez	Portland General Electric Company	X		X		X	X				
23.	Individual	Martin Bauer	US Bureau of Reclamation					X					
24.	Individual	Terrence Walsh	Consolidated Edison Company of New York INC.	X		X		X					
25.	Individual	Edward Bedder	Orange and Rockland Utilities Inc	X									
26.	Individual	Greg Rowland	Duke Energy	X		X		X	X				
27.	Individual	Roger Champagne	Hydro-Québec TransEnergie (HQT)	X									
28.	Individual	Dan Rochester	Independent Electricity System Operator		X								
29.	Individual	Jason Shaver	American Transmission Company	X									

1. In its order approving CIP-002-2 through CIP-009-2, the Commission directed NERC to make changes to CIP-006-2 and CIP-008-2 as well as the implementation plan for newly identified critical cyber assets and file those changes within 90 days of the order. Do you agree that the SAR accurately addresses the scope of these directives? If not, please identify what you feel is missing in the SAR.

Summary Consideration:

About a quarter of the respondents provided comments on the SAR and its accurate representation of the FERC Order approving Version 2 CIP Standards issued September 30, 2009, which included direction to: add a requirement for a visitor control program (CIP-006); remove the statement regarding the removal of a component or system from service as part of the incident response plan test (CIP-008); and update the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities.

Many comments were positive that the SAR accurately reflected the Commission's directives. Concerns were raised regarding the impact of a visitor control program in CIP-006, especially with field operations, requiring visitors to sign in and out every time a physical security perimeter is crossed, and be escorted. These issues were clarified by the SDT in its responses.

Other comments applauded the SDT for following the standard development process and preparing a compliance filing in an extremely shortened timeframe.

The current revisions to the CIP-006 and CIP-008 standards and the implementation plans were given a very high priority by FERC. In response, the Cyber Security Order 706 standard drafting team re-organized its resources and schedule, and together with the industry, made the effort to incorporate the directed changes while following the NERC standard development process in a compressed timeframe.

The SDT made the following modification to the CIP standards, based on stakeholder comments:

Revised the CIP-006 R1.6 requirement as shown below to more closely address the specific directives included in the FERC Order approving Version 2 CIP Standards issued September 30, 2009.

R1.6. A visitor control program for visitors (personnel without authorized unescorted access to a Physical Security Perimeter), containing at a minimum the following:

R1.6.1. Logs (manual or automated) to document the entry and exit of visitors, including the date and time, to and from Physical Security Perimeters.

R1.6.2. Continuous escorted access of visitors within the Physical Security Perimeter.

Organization	Yes or No	Question 1 Comment
NextEra Energy Resources	No	Generally we agree with the proposed changes. However, one area of concern is CIP-006-2. We feel that it should not be a requirement for persons with unescorted physical access to have to swipe out when leaving the PSP. Swiping in should be sufficient.
Response: The SDT clarifies that Requirement CIP-006 R1.6 specifies a visitor control program. The SDT did not modify the requirements for individuals with authorized unescorted access to the Physical Security Perimeter. CIP-006 R6 requires a log that captures "time of access" for all individuals who enter a Physical Security Perimeter. Project 2008-15 "Interpretation of CIP-006-1a By US Army Corps of Engineers" clarifies that the term "time of access" indeed refers to the time an authorized individual enters the physical security perimeter.		
Florida Power & Light	No	Generally we agree with the proposed changes. However, one area of concern is CIP-006-2. We feel that it should not be a requirement for persons with unescorted physical access to have to swipe out when leaving the PSP. Swiping in should be sufficient.
Response: The SDT clarifies that Requirement CIP-006 R1.6 specifies a visitor control program. The SDT did not modify the requirements for individuals with authorized unescorted access to the Physical Security Perimeter. CIP-006 R6 requires a log that captures "time of access" for all individuals who enter a Physical Security Perimeter. Project 2008-15 "Interpretation of CIP-006-1a By US Army Corps of Engineers" clarifies that the term "time of access" indeed refers to the time an authorized individual enters the physical security perimeter.		
Portland General Electric Company	No	
American Transmission Company	Yes	ATC agrees that the SAR reflects the Commission's directive but we do not agree with all of the proposed changes. (Please see our specific comments in the other questions.)
Response: Thank you for your comments		
US Bureau of Reclamation	Yes	We applaud the SDT in following the standards development process by submitting an implementaton plan that addresses the Commissions order. This is consistent with the Commissions requirement that "We direct NERC to submit, within 90 days of the date of issuance of this order, a compliance filing that includes a revised Version 2 Implementation Plan, addressing the Version 2 CIP Reliability Standards, that clarifies the matters specified in the attachment to this order" it is also consistent with the process for submitting revision (Reference 16 USC Sec. 824o (d) (5) The Commission, upon its own motion or upon complaint, may order the Electric Reliability Organization to submit to the Commission a proposed reliability standard or a modification to a reliability standard that addresses a specific matter if the Commission considers such a new or modified reliability standard appropriate to carry out this section.)

Organization	Yes or No	Question 1 Comment
Response: Thank you for your comments		
FirstEnergy	Yes	We commend NERC for their expedient response to FERC's directives.
Response: Thank you for your comments		
San Diego Gas and Electric Co	Yes	While the SAR does accurately address the scope of the FERC directives, we would suggest that the SAR's name be changed to something more descriptive than "Cyber Security Ninety-Day Response" to make it easier to locate and understand in the future. Perhaps a SAR title like "NERC response to FERC Cyber Security V2 Std Approval" would help to make the contents clearer when searching or browsing in the future.
Response: Thank you for your comments. We will submit the suggestion for future Project Naming.		
American Electric Power	Yes	
BGE CIP Core Team	Yes	
Bonneville Power Administration	Yes	
Consolidated Edison Company of New York INC.	Yes	
Dominion Virginia Power	Yes	
Duke Energy	Yes	
E.ON U.S. LLC	Yes	
Exelon	Yes	
Hydro-Québec TransEnergie (HQT)	Yes	
Independent Electricity System	Yes	

Organization	Yes or No	Question 1 Comment
Operator		
Manitoba Hydro	Yes	
MidAmerican Energy Company	Yes	
Midwest ISO Standards Collaborators	Yes	
Navasota Odessa Energy Partners, LP	Yes	
Northeast Power Coordinating Council	Yes	
Orange and Rockland Utilities Inc	Yes	
PacifiCorp	Yes	
PJM Interconnection	Yes	
Silicon Valley Power	Yes	
South Carolina Electric and Gas	Yes	
The United Illuminating Company	Yes	

2. Do you agree that the proposed modifications to CIP-006-2, CIP-008-2, and the implementation plans meet the intent of the Commission's directives? If not, please identify what changes you feel are needed to meet the intent of these directives.

Summary Consideration:

About half of the respondents provided feedback regarding the proposed modifications to CIP-006, CIP-008, and the Implementation Plans to meet the intent of the Commission's directives. The majority of the issues that were raised concerned the requirements associated with the visitor control program and the Implementation Plan requirements. The commenters suggested that the visitor control program requirements stated in CIP-006 may have gone beyond the directive from FERC in its Order approving Version 2 CIP Standards issued September 30, 2009 by requiring the documentation of visitor identity, purpose of visit, time and date of entry and exit from physical security perimeters, and the identity of the escort since this may go beyond the readily available technology of badging systems, especially in field locations.

Many commenters were concerned that the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities includes language stating that the first occurrence of a recurring requirement must be completed by the Compliant milestone date. Others were looking for guidance on the treatment of newly acquired assets if acquired from a third party.

These requirements were clarified by the SDT in its responses. The comments on the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities were considered by the SDT and determined to be more of a compliance issue that would be more appropriately addressed by NERC Compliance staff. The language concerning the required date of compliance in the Implementation Plan was removed and the issue referred.

The SDT made the following modification to the standard, based on stakeholder comments:

- Revised the language in CIP-006 R1.6 to not be overly prescriptive in defining the requirements for the visitor control program. (See the Summary Consideration for question 1 for the specific changes.)
- Removed the following language from the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities concerning the date of first occurrence of a recurring requirement – the NERC Compliance Staff is expected to issue a compliance bulletin addressing this issue:

> A number of the NERC Reliability Standard requirements include a prescribed periodicity or recurrence of the requirement activity (e.g., an annual review of documentation). In those instances, the first occurrence of the recurring requirement must be completed by the Compliant milestone date in Table 2. The entity is then required to collect and maintain required "data," "documents," "documentation," "logs," and "records" to demonstrate compliance with the recurring requirement after the Compliant milestone date has been reached.

For those NERC Reliability Standard requirements that include a prescribed records retention period (e.g., retention of logs for 90 days), a Responsible Entity is expected to begin collection and retention of the required "data," "documents," "documentation," "logs," and "records" by the Compliant milestone date in Table 2.

For retention requirements that are triggered by a specific event (e.g., a reportable incident), collection and retention of the required "data," "documents," "documentation," "logs," and "records" begins with the triggering event. In this instance, the requirement for records collection and retention does not begin until the Compliant milestone date in Table 2 is reached and only applies to triggering events occurring after the Compliant milestone date.

For those NERC Reliability Standard requirements that do not include a specified periodicity or records retention requirement, a Responsible Entity is expected to have available all records required to demonstrate compliance to these requirements by the Compliant milestone date in Table 2.

Organization	Yes or No	Question 2 Comment
Consolidated Edison Company of New York INC.	No	CIP-006 R1.6.1 is not consistent with the FERC Order. Recommend using the Commission's Determination – "Such logs can provide auditable records that identify visitors, the purpose of the visit, date and time of entry and exit, and who escorted the visitor." We suggest: "R1.6.1. Visitor logs (manual or automated) to identify visitors, the purpose of the visit, the date and time of entry and exit from the Physical Security Perimeters, and to identify personnel with authorized, unescorted physical access performing the escort." CIP-006 R1.6.2 should be modified to "R1.6.2. Requirement for continuous escorted access of visitors within the Physical Security Perimeter." The Implementation for Newly Identified Critical Cyber Assets and Newly Registered Entities says "In those instances, the first occurrence of the recurring requirement must be completed by the Compliant milestone date in Table 2." We do not agree since the initial Implementation Plan expected the initial review to occur after the Compliant milestone and before the Auditably Compliant milestone. These words are not in any FERC Order or Directive. For more information see the answer to question 4.

Response:

CIP-006 R1.6.1:

The Commission discussed elements of a common visitor log as highlighted in the comment. However, the Commission directive only specified the use of visitor logs to document entry and exit. The standard drafting team has made the modifications to be consistent with the FERC directive.

The elements of the visitor log selected by the SDT represent a baseline for an acceptable visitor log and entities are free to exercise their flexibility in

Organization	Yes or No	Question 2 Comment
implementing a more rigorous visitor log if they so choose. **CIP-006 R1.6.2:** **The SDT agrees that the modification to CIP-006 R1.6.2 adds clarity and does not modify the intent. CIP-006 R1.6.2 has been modified as suggested.** **Implementation Plan:** **Regarding the Implementation Plan for Newly Identified Critical Assets and Newly Registered Entities, the Standard Drafting Team has considered comments on this issue and has determined that this is a compliance issue that is inappropriately addressed in this Implementation Plan. The paragraph will be removed in the amended plan and the appropriate adjustments will be made where this issue is referenced elsewhere in the Plan.** **The SDT acknowledges that the initial performance date of tasks being performed as part of meeting recurring requirements is problematic from an audit perspective. The SDT also acknowledges that this issue is not confined to the CIP standards alone and hence the impact of this comment (by its nature) goes beyond the scope of this SDT. The NERC Compliance Staff is expected to issue a compliance bulletin addressing this issue.**		
Hydro-Québec TransEnergie (HQT) Independent Electricity System Operator Northeast Power Coordinating Council	No	CIP-006 R1.6.1 is not consistent with the FERC Order. Recommend using the Commission's Determination – "Such logs can provide auditable records that identify visitors, the purpose of the visit, date and time of entry and exit, and who escorted the visitor." CIP-006 R1.6.2 should be modified to "Requirement for continuous escorted access of visitors within the Physical Security Perimeter." The Implementation for Newly Identified Critical Cyber Assets and Newly Registered Entities says "In those instances, the first occurrence of the recurring requirement must be completed by the Compliant milestone date in Table 2." We do not agree since the initial Implementation Plan expected the initial review to occur after the Compliant milestone and before the Auditably Compliant milestone. These words are not in any FERC Order or Directive. For additional information see the response to question 4.
Response: **CIP-006 R1.6.1:** **The Commission discussed elements of a common visitor log as highlighted in the comment. However, the Commission directive only specified the use of visitor logs to document entry and exit. The standard drafting team has made the modifications to be consistent with the FERC directive.** **The elements of the visitor log selected by the SDT represent a baseline for an acceptable visitor log and entities are free to exercise their flexibility in implementing a more rigorous visitor log if they so choose.**		

Organization	Yes or No	Question 2 Comment
CIP-006 R1.6.2: **The SDT agrees that the modification to CIP-006 R1.6.2 adds clarity and does not modify the intent. CIP-006 R1.6.2 has been modified as suggested.** **Implementation Plan:** **Regarding the Implementation Plan for Newly Identified Critical Assets and Newly Registered Entities, the Standard Drafting Team has considered comments on this issue and has determined that this is a compliance issue that is inappropriately addressed in this Implementation Plan. The paragraph will be removed in the amended plan and the appropriate adjustments will be made where this issue is referenced elsewhere in the Plan.** **The SDT acknowledges that the initial performance date of tasks being performed as part of meeting recurring requirements is problematic from an audit perspective. The SDT also acknowledges that this issue is not confined to the CIP standards alone and hence the impact of this comment (by its nature) goes beyond the scope of this SDT. The NERC Compliance Staff is expected to issue a compliance bulletin addressing this issue.**		
Orange and Rockland Utilities Inc	No	CIP-006 R1.6.1 is not consistent with the FERC Order. Recommend using the Commission's Determination - Such logs can provide auditable records that identify visitors, the purpose of the visit, date and time of entry and exit, and who escorted the visitor. We suggest: R1.6.1. Visitor logs (manual or automated) to identify visitors, the purpose of the visit, the date and time of entry and exit from the Physical Security Perimeters, and to identify personnel with authorized, unescorted physical access performing the escort. CIP-006 R1.6.2 should be modified to R1.6.2. Requirement for continuous escorted access of visitors within the Physical Security Perimeter. The Implementation for Newly Identified Critical Cyber Assets and Newly Registered Entities says "In those instances, the first occurrence of the recurring requirement must be completed by the Compliant milestone date in Table 2." We do not agree since the initial Implementation Plan expected the initial review to occur after the Compliant milestone and before the Auditably Compliant milestone. These words are not in any FERC Order or Directive. For more information see the answer to question 4.
Response: **The Commission discussed elements of a common visitor log as highlighted in the comment. However, the Commission directive only specified the**		

Organization	Yes or No	Question 2 Comment
use of visitor logs to document entry and exit. The standard drafting team has made the modifications to be consistent with the FERC directive. **The elements of the visitor log selected by the SDT represent a baseline for an acceptable visitor log and entities are free to exercise their flexibility in implementing a more rigorous visitor log if they so choose.** **CIP-006 R1.6.2:** **The SDT agrees that the modification to CIP-006 R1.6.2 adds clarity and does not modify the intent. CIP-006 R1.6.2 has been modified as suggested.** **Implementation Plan:** **Regarding the Implementation Plan for Newly Identified Critical Assets and Newly Registered Entities, the Standard Drafting Team has considered comments on this issue and has determined that this is a compliance issue that is inappropriately addressed in this Implementation Plan. The paragraph will be removed in the amended plan and the appropriate adjustments will be made where this issue is referenced elsewhere in the Plan.** **The SDT acknowledges that the initial performance date of tasks being performed as part of meeting recurring requirements is problematic from an audit perspective. The SDT also acknowledges that this issue is not confined to the CIP standards alone and hence the impact of this comment (by its nature) goes beyond the scope of this SDT. The NERC Compliance Staff is expected to issue a compliance bulletin addressing this issue.**		
San Diego Gas and Electric Co	No	CIP-008-2: We are in agreement with the proposed modifications to CIP-008-2. CIP-006-2: In the modifications made to CIP-006-2, we have an issue with the language requiring the documentation of "entry to and exit from Physical Security Perimeters." Many badging systems document personnel ingress to PSP areas, but not egress and some entities may utilize their badging system to track visitors (visitors swipe for record keeping purposes but their badge cannot open any access points). A recent interpretation of CIP-006 also confirmed that only ingress monitoring is required, and that is the functionality delivered by many badge access systems. After their visit is completed, a visitor typically signs out at the central Security Station and surrender their visitor badge at that time. In order to make the R1.6 language more easily understood, our first preference would be to remove the "and exit from" language. If that cannot be done, then our second preference would be to change the language in R1.6.1 to "date of entry to and last exit of the day from Physical Security Perimeters". Manually logging all visitor ingress and egress from CCA areas could be potentially very time-consuming without providing additional reliability to the Bulk Electric System. Implementation Plans:

Organization	Yes or No	Question 2 Comment
		In the Implementation plan language, we were looking for particular guidance showing how an asset would be treated if acquired from a third party. In particular, there could be a scenario where the current owner does not list any critical assets or critical cyber assets. Once the acquisition takes place, what accommodations should be made in the implementation plan if the new owner feels that there are critical assets or critical cyber assets associated with the asset? It could theoretically take a considerable amount of time to start a proper Cyber Security program for the acquired plant from scratch. A 12 month implementation plan schedule may not be practical given the complexity of assessing the acquired plant and making the necessary cyber security modifications and additions for Compliance. We'd like to suggest that a 24 month implementation plan schedule would be more appropriate in cases like this.

Response:

CIP-008-2:

Thank you for your comment

CIP-006-2:

The SDT does not agree that the requirement forces a very time-consuming process on the entity in logging the ingress and egress of visitors from Physical Security Perimeters. It is the opinion of the SDT that documenting precisely when unauthorized individuals had escorted access inside Physical Security Perimeters is a key element of a strong visitor control program. The SDT reminds the entity that it also has the discretion to grant an individual authorized unescorted physical access to the Physical Security Perimeter should the requirement of escorting and logging ingress and egress prove burdensome.

Implementation Plan:

- **Where the third party did not identify this asset as a critical asset and did not have a CIP compliance program in place for the acquired asset, if the current owner does not list any critical assets or critical cyber assets, and as a result of the acquisition of the asset, it has one year from the date of the acquisition to merge the CIP programs and conduct its risk-based methodology, or at the required one year review of its application of the CIP-002 Critical Asset risk-based methodology since the last application, whichever is earlier. The scenario indicates that the application of the methodology now determines that this is a newly identified Critical Asset. Under the Implementation Plan, the newly identified Critical Asset's implementation of the CIP program falls under category 1 and the entity has 24 months from the date of the identification of the Critical Asset with Critical Cyber Assets to implement its CIP program for these Critical Cyber Assets, as per the Category 1 column of Table 2. This is explained in the Newly Registered Entity Scenario 1 (Application of Category 1 of the Implementation Plan, "A Merger of Two or More Registered Entities where None of the Predecessor Registered Entities has Identified any Critical Cyber Asset," Page 8.**

- **Where the third party has identified the acquired asset as a Critical Asset containing Critical Cyber Assets prior to the acquisition and therefore had a CIP program for these cyber assets, the CIP program can independently be operated and the entity has one year to decide whether to merge the programs under a single Senior Manager. In either case, the CIP program is already effective and applicable upon**

Organization	Yes or No	Question 2 Comment
acquisition. This is explained under Newly Registered Entity Scenario 1 (Application of Category 2, "A Merger of Two or More Registered Entities where Only One of the Predecessor Registered Entities has Identified at Least One Critical Cyber Asset," Page 9.		
E.ON U.S. LLC	No	In paragraph 29 of the Order, the Commission approves version 2 of the standard on the basis that continuous is analogous to supervised. Furthermore, the Commission states as its goal that Responsible Entities implement visitor control programs and be able to reasonably demonstrate that they maintain such programs. The order reiterates that the Version 2 standards achieve this goal. The proposed changes to CIP-006-2 do not meet the Commission's goal because of prescriptive measures that do not allow for reasonable demonstration
Response: The modifications to CIP-006 were made in direct response to paragraph 30 of the FERC Order approving the Version 2 CIP Standards issued September 30, 2009. Respectfully, the SDT does not agree that the requirement to implement a visitor control program is overly prescriptive or that it cannot be reasonably demonstrated. 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).		
NextEra Energy Resources Silvia Parada-Mitchell Florida Power & Light	No	In reading the second sentence of the New Asset Implementation Plan redline which starts, "In those instances?" it seems that this is stating that an entity must demonstrate compliance prior to the actual Compliant date set forth in the current implementation plan. The implementation plan right now states that the period of time between the Compliant date and Auditably Compliant date is when you must start keeping records, logs, documents, etc. If the current proposal goes through, the entity would need to conduct its first vulnerability assessment sometime prior to the Compliant date. This is a huge shift and shortens the implementation window up to a year. Hence, we feel this change should not be approved.
Response: Thank you for your comment **Regarding the Implementation Plan for Newly Identified Critical Assets and Newly Registered Entities, the Standard Drafting Team has considered comments on this issue and has determined that this is a compliance issue that is inappropriately addressed in this Implementation Plan. The paragraph will be removed in the amended plan and the appropriate adjustments will be made where this issue is referenced elsewhere in the Plan.** **The SDT acknowledges that the initial performance date of tasks being performed as part of meeting recurring requirements is problematic from an audit perspective. The SDT also acknowledges that this issue is not confined to the CIP standards alone and hence the impact of this comment (by its nature) goes beyond the scope of this SDT. The NERC Compliance Staff is expected to issue a compliance bulletin addressing this issue.**		
Manitoba Hydro	No	The Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities was modified beyond the Commision's directives in RD09-7-000. See response to Question 4.

Organization	Yes or No	Question 2 Comment
Response: Thank you for your comment. The Standards Drafting Team has responded to your comments in its response to Question 4, below.		
Exelon	No	We do not agree with the CIP-006-3 R1.6 change where you have included the requirement for the visitor log to contain "...the identity of personnel with authorized, unescorted physical access performing the escort." This would be an excessive administrative burden that goes beyond what FERC ordered in paragraph 30 which simply stated "...the commission directs the ERO to develop a modification to Reliability Standard CIP-006-2, through the NERC Reliability Standards development process, to add a requirement on visitor control programs, including the use of visitor logs to document entry and exit, within 90 days of the date of this order". Your additional requirement can be interpreted to mean any hand off of escort responsibilities would also need to be documented which would be an excessive administrative burden that would provide no additional assurances or security. An acceptable alternative would be for the visitor log to include a reference to the site contact and reason for the visit. These are things known at the time of visitor sign in which would not require additional updates through out the time the visitor remains within the secure area.
Response: CIP-006 R1.6.1: **The Commission discussed elements of a common visitor log as highlighted in the comment. However, the Commission directive only specified the use of visitor logs to document entry and exit. The standard drafting team has made the modifications to be consistent with the FERC directive.** **The elements of the visitor log selected by the SDT represent a baseline for an acceptable visitor log and entities are free to exercise their flexibility in implementing a more rigorous visitor log if they so choose.**		
Portland General Electric Company	No	
American Transmission Company	Yes	ATC does not agree with the deletion of the following sentence from CIP-008-2 R1.6 “Testing the Cyber Security Incident response plan does not require removing a component or system from service during the test”. Although, ATC believes that FERC is correct in its assessment that the sentence could be inferred by Requirement 1 and Requirement 1.6, it does not harm the requirement in any way by remaining part of the standard and should not be deleted. The Commission goes as far as to say that the sentence is similar to an interpretation, so, if that is the case, we don’t see any harm in keeping it as part of the standard. Lastly, ATC is concerned that we could be back to this same spot if an entity requests a formal definition of this requirement. From the SDT perspective, what issues are being addressed by removing this sentence? Does the SDT believe that the deletion of this specific sentence will not require the removal of equipment in order to be in compliance with the standard? ATC believes that the sentence does provide additional clarity of the requirements and does not harm reliability and, therefore, should not be removed from the standard. As the Commission clearly points out, this sentence does provide an interpretation or clarification of the standard

Organization	Yes or No	Question 2 Comment
		which the Commission did not disagree. If the SDT does remove this sentence, then we request the SDT to identify any concerns or issues with the interpretation or clarification. (Deleted Sentence) Specifically, would the SDT give an alternate interpretation of this requirement?
Response: In response to the FERC Order 706, the SDT understood that FERC had provided direction in par. 687, "the Commission clarifies that, with respect to full operational testing under CIP-008-1, such testing need not require a responsible entity to remove any systems from service. The ERO should clarify this in the revised Reliability Standard and may use a term different than full operational exercise", which required the inclusion of the statement. Subsequently, in the FERC Order approving the Version 2 CIP Standards issued September 30, 2009, the Commission directed NERC to remove this statement and stated in their determination that "we did not see a need to modify the Reliability Standard merely to add this point and we did not direct NERC to make such a modification. Moreover, this point is not a requirement, but rather, is similar to an interpretation or clarification of a requirement". **This statement was additional information, not a requirement, whose inclusion or removal from the standard does not affect the implementation of the requirement, and can be removed. The language of the requirement does not require removal of equipment from service. This information could be included in future guidance documentation. The SDT is not aware of any issues with this clarification.**		
South Carolina Electric and Gas	Yes	Order No. 706-B Nuclear Implementation schedule should be added to the implementation table for the proposed modifications to CIP-006-2, CIP-008-2 in order to avoid any confusion between the two schedules.
Response: The Version 2 and Version 3 CIP Standards implementation is independent of the 706B implementation plan. Specifically, the Version 2 implementation date is 4/1/10. The first milestone under the 706B implementation plan is 12 months following FERC approval, which is after 4/1/10, and likely into 2011.		
American Electric Power	Yes	
BGE CIP Core Team	Yes	
Bonneville Power Administration	Yes	
Dominion Virginia Power	Yes	
Duke Energy	Yes	
FirstEnergy	Yes	

Organization	Yes or No	Question 2 Comment
MidAmerican Energy Company	Yes	
Midwest ISO Standards Collaborators	Yes	
Navasota Odessa Energy Partners, LP	Yes	
PacifiCorp	Yes	
PJM Interconnection	Yes	
Silicon Valley Power	Yes	
The United Illuminating Company	Yes	
US Bureau of Reclamation	Yes	

3. Do you have any additional comments associated with the proposed SAR for Project 2009-21: Cyber Security Ninety-day Response? If yes, please explain.

Summary Consideration:

About a third of the respondents provided additional comments and feedback concerning the proposed SAR for Project 2009-21: Cyber Security Ninety-day Response. A number of comments addressed the respondents' concern of not following the approved SAR process in the development and implementation of this SAR. The concerns were related to the potential for introduction of ambiguity and not having the time to openly discuss the issues that the SAR is addressing. The perception was that the imposition of an unreasonably short schedule threatens to undermine the standards development process being followed by NERC.

Organization	Yes or No	Question 3 Comment
American Electric Power	No	
American Transmission Company	No	
BGE CIP Core Team	No	
Bonneville Power Administration	No	
Dominion Virginia Power	No	
Duke Energy	No	
E.ON U.S. LLC	No	
Exelon	No	
Manitoba Hydro	No	
MidAmerican Energy Company	No	

Organization	Yes or No	Question 3 Comment
Navasota Odessa Energy Partners, LP	No	
PJM Interconnection	No	
Portland General Electric Company	No	
Progress Energy	No	
San Diego Gas and Electric Co	No	
Silicon Valley Power	No	
South Carolina Electric and Gas	No	
The United Illuminating Company	No	
US Bureau of Reclamation	No	
NextEra Energy Resources Florida Power & Light	Yes	Although the SAR proposes many changes, these changes lead to ambiguity and this ambiguity lends more latitude to the regions.
Response: Thank you for your comment. The changes proposed in the SAR were in response to the FERC directive.		
PacifiCorp	Yes	Comments: PacifiCorp generally supports the Request for Rehearing or Clarification submitted by the Edison Electric Institute (EEI) submitted in FERC Docket No. RD09-7 on October 30, 2009. Specifically, PacifiCorp agrees with EEI that the ninety-day deadline imposed by FERC's September 30, 2009 to modify the CIP Reliability Standards is unreasonably short. In addition, PacifiCorp is concerned that this type of unreasonable deadline threatens to undermine NERC's standards development process. Currently, the NERC standards development process is the only opportunity for industry stakeholders to participate in the development of reliability standards that will have significant operational and business impacts. Unreasonable deadlines set by FERC and the corresponding "expedited" standards development process threatens to undermine the robustness of the current process. While PacifiCorp does not have substantive issues with the current proposed changes, it is concerned regarding the procedure being used here to adopt

Organization	Yes or No	Question 3 Comment
		these changes.
Response: The drafting team asked the Standards Committee to approve use of the "Urgent Action" standard development process so that the team could address the directives without requesting a variance from the standards process. Under the "Urgent Action" process, a SAR and proposed standard (and implementation plan) are all posted at once for a 30-day pre-ballot review, followed by the initial ballot. The Standards Committee directed the drafting team to post the SAR and proposed standard for a 30-day comment period, followed as quickly as practical by the initial ballot. In making this decision, the Standards Committee was attempting to provide respondents with an opportunity to provide comment on the proposed modifications before proceeding to ballot. Posting a SAR with a proposed standard is not a violation of the standards development process – this is allowed. The Standards Committee reports to the NERC Board of Trustees and has dual obligations – to protect the integrity of the standards process and to assist NERC in meeting its obligations as the ERO.		
Consolidated Edison Company of New York INC. Hydro-Québec TransEnergie (HQT) Independent Electricity System Operator Northeast Power Coordinating Council	Yes	Development of this SAR should follow the approved SAR process
Response: The drafting team asked the Standards Committee to approve use of the "Urgent Action" standard development process so that the team could address the directives without requesting a variance from the standards process. Under the "Urgent Action" process, a SAR and proposed standard (and implementation plan) are all posted at once for a 30-day pre-ballot review, followed by the initial ballot. The Standards Committee directed the drafting team to post the SAR and proposed standard for a 30-day comment period, followed as quickly as practical by the initial ballot. In making this decision, the Standards Committee was attempting to provide respondents with an opportunity to provide comment on the proposed modifications before proceeding to ballot. Posting a SAR with a proposed standard is not a violation of the standards development process – this is allowed. The Standards Committee reports to the NERC Board of Trustees and has dual obligations – to protect the integrity of the standards process and to assist NERC in meeting its obligations as the ERO.		
FirstEnergy	Yes	We understand that NERC is merely responding to directives with a specific completion time frame of 90-days. And we believe that NERC has done this job well. Unfortunately, due to the short 90-day time frame, NERC and its stakeholders did not have much time to challenge FERC's directives. We offer the following as strictly comments on the directive to modify CIP-008: CIP-008 Req. R1.6

Organization	Yes or No	Question 3 Comment
		FERC feels that the statement "Testing the Cyber Security Incident response plan does not require removing a component or system from service during the test" should be removed and NERC has proposed to remove it per the directive by FERC. It is interesting to note that in Order 706 par. 687, FERC stated "the Commission clarifies that, with respect to full operational testing under CIP-008-1, such testing need not require a responsible entity to remove any systems from service. The ERO should clarify this in the revised Reliability Standard and may use a term different than full operational exercise" Yet, in the recent Order, per par. 38, FERC has directed NERC to remove this statement and stated in their determination "we did not see a need to modify the Reliability Standard merely to add this point and we did not direct NERC to make such a modification. Moreover, this point is not a requirement, but rather, is similar to an interpretation or clarification of a requirement". It appears that FERC may have inadvertently sent unclear and inconsistent messages when it said "the ERO should clarify" in Order 706, and then asked NERC to remove the statement in the recent Order because it is merely a "clarification of the requirement". It is not clear how removing this statement makes R1.6 a better requirement since, as FERC says, "...it is similar to an interpretation or clarification of a requirement." In addition, the phrase, "A test of the Cyber Security Incident response plan can range from a paper drill, to a full operational exercise..." is also a clarifying statement and the FERC raised no concern over its inclusion in this standard requirement. The direction to remove clarifying statements seems to go against the goal of writing clear and concise reliability standards.
Response: In response to the FERC Order 706, the SDT understood that FERC had provided direction in par. 687, "the Commission clarifies that, with respect to full operational testing under CIP-008-1, such testing need not require a responsible entity to remove any systems from service. The ERO should clarify this in the revised Reliability Standard and may use a term different than full operational exercise", which required the inclusion of the statement. Subsequently, in the FERC Order approving the Version 2 CIP Standards issued September 30, 2009, the Commission directed NERC to remove this statement and stated in their determination that "we did not see a need to modify the Reliability Standard merely to add this point and we did not direct NERC to make such a modification. Moreover, this point is not a requirement, but rather, is similar to an interpretation or clarification of a requirement". **This statement was additional information, not a requirement, whose inclusion or removal from the standard does not affect the implementation of the requirement, and can be removed. The language of the requirement does not require removal of equipment from service. This information could be included in future guidance documentation. The SDT is not aware of any issues with this clarification.**		
Midwest ISO Standards Collaborators	Yes	While we agree that the SDT has addressed the concerns identified by the Commission in the FERC order, we do not believe the changes are closing a significant gap in reliability. At best, these changes simply expand upon the understanding of what the continuous escort requirement means. Thus, these changes do not warrant violating the Commission approved Reliability Standards Development Process by combining the commenting and pre-ballot review periods. The end result is that the Cyber Security - 706 Order standards drafting team has to divert their scarce resources from focusing on developing the next generation of the CIP

Organization	Yes or No	Question 3 Comment
		standards to this fire drill exercise to make a small incremental improvement to the standard. There is no reason these changes could not have been addressed in the process of developing the next generation of CIP standards.
Response: The SDT understands and appreciates your concerns, but issues regarding FERC's imposed timeline cannot be addressed in response to comments.		
Orange and Rockland Utilities Inc	Yes	

4. Do you have any additional comments associated with the proposed CIP-006-2, CIP-008-2, and the implementation plans? If yes, please explain.

Summary Consideration:

Nearly all of the respondents provided comments to the proposed CIP-006-2, CIP-008-2, and Implementation Plan Requirements. The majority of the issues that were raised concerned the respondents' need for a better understanding of the Implementation Plan requirements.

Many comments referred to the language concerning the start date for demonstration of compliance with recurring requirements. Other significant comments addressed the prescriptive nature of the requirements for the visitor control program and the treatment of combined assets from merged or acquired Registered Entities.

The SDT made no additional modifications to the standards and implementation plan requirements, based on these respondent comments.

Organization	Yes or No	Question 4 Comment
Exelon	No	1) For the "Implementation Plan for "Newly Registered Entities", we suggest the that the last two sentences in the second paragraph under the Category 1 Scenario beginning with following language should be deleted: "it would be preferred that a single program be the result of this analysis, however". 2) For the "Implementation Plan for "Newly Registered Entities", we suggest that the last two sentences of the Scenario 3, (a) paragraph be deleted: "It would be preferred that a single program be the result of this analysis, however, Registered Entity specific circumstances may dictate or allow the two programs to continue separately. These decisions may be subject to review as part of compliance with NERC Reliability Standard CIP-002."
Response: Thank you for your comments **1) This statement in the Implementation Plan is not a requirement. The statement is intended to provide guidance. It is the opinion of the SDT that a single program reduces complexity for both the Responsible Entity and the compliance monitoring and enforcing organizations.** **2) This statement in the Implementation Plan is not a requirement. The statement is intended to provide guidance. It is the opinion of the SDT that a single program reduces complexity for both the Responsible Entity and the compliance monitoring and enforcing organizations. Further, it reinforces that "Registered Entity specific circumstances may dictate or allow the two programs to continue separately."**		
American Electric Power	No	
Bonneville Power Administration	No	

Organization	Yes or No	Question 4 Comment
Navasota Odessa Energy Partners, LP	No	
San Diego Gas and Electric Co	No	
South Carolina Electric and Gas	No	
The United Illuminating Company	No	
US Bureau of Reclamation	No	
BGE CIP Core Team	Yes	1. 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)? 2. What is the implementation plan for the CIP Version 3 Reliability Standards?
Response: **1) The SDT leaves the specific details of interpreting the standards to their unique environment up to the entity.** **2) The "Implementation Plan for Version 3 of Cyber Security Standards CIP-002-3 through CIP-009-3" says that "The Responsible Entities shall be compliant with all requirements on the Effective Date specified in each standard". Under Proposed Effective Date, end of Page 1, the current Proposed Effective Date in each standard for Version 3 specifies: "The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required)."**		
FirstEnergy	Yes	CIP-007 Per NERC Project 2009-16, the stakeholders and NERC's Board recently approved an interpretation of Req. R2 to clarify that the meaning of ports in this requirement is referring to "logical" ports. NERC may want to consider adding this interpretation to CIP-007 Version 3 so that it gets incorporated into the standard expediently rather than wait until a later time. Waiting until a later time will require both another revision to the standard and an extra filing by NERC to add the interpretation.
Response: The drafting team limited its modifications to CIP-007 to just those conforming changes needed for accuracy in identifying associated standards - no changes were made to any of the requirements in this set of standards to incorporate interpretations. The interpretation of CIP-007 for		

Organization	Yes or No	Question 4 Comment
WECC was approved by the BOT on November 5, 2009 and has not been filed for regulatory approvals. Interpretations do not become effective until approved by regulatory authorities. **Note that the interpretation becomes linked to the standard it clarified - and in this case will need to be carried forward and attached to later versions of the same standard if the requirement remains the same in each version.**		
PJM Interconnection	Yes	Comments: PJM would like to request clarification on the meaning of "identity" in CIP 006-3, Requirement R1.6.1; "Visitor logs to document visitor's identity, time and date of..." It is not clear, if the logs should only contain the visitor's name or it should require some form of verification of his/her identity, such as, a government (federal or local) issue photo ID. PJM is in agreement with a "Medium" VRF for standard number "CIP-006-3a", Requirement number "R1.6.1", if the clarification of "identity" represents the verification of the individuals identity; however, if the clarification of "identity" means, that the log should only contain "name only", PJM suggest the VRF of "Low".
Response: **The SDT agrees that there was some confusion around this issue and has modified the standard requirement to more closely align with the FERC order. See the summary consideration in response to question 1 to see how R1.6.1 was changed. (Page 7 of this report)** **It is the opinion of the SDT that 'facilities security' is critically important, as also indicated by the Commission, and that visitor control programs and visitor logs are an essential element of sound facilities security. Therefore, it is the opinion of the SDT that a VRF of "Medium" is appropriate for R1.6.1.**		
American Transmission Company	Yes	Implementation Plan Comments: Item 1: What does the word "compliant" mean when used in the phrase "when Registered Entities has been required to be compliant with NERC Reliability Standard CIP-002"? Does the team mean the "compliant" phase identified in the Original CIP Implementation plan? or, Does the team mean when an entity had to be either "substantially compliant" or "auditable compliant"? The Version 1 Implementation plan identifies three compliant phases. Substantially Compliant, Compliant, and Auditably Compliant. Item 2: Question about the last paragraph on page 3: (For example, if a particular transmission substation has been designated??)This example is structured around the premise that an entity has identified a Critical Asset but has not identified any associated Critical Cyber Asset and seems to point to scenario 3. Is this an example for scenario 3? If so, the SDT should insert an affirmative sentence linking it to scenario 3. Item 3:Question about paragraph 2 on page 4: (If, however, a particular transmission substation with Cyber Assets does not) What scenario (1, 2 or 3) is this paragraph attempting to address? It seems that it may be

Organization	Yes or No	Question 4 Comment
		attempting to provide an example of scenario 2 and, if so, we would suggest that the SDT provide a specific sentence linking it to a specific scenario. Item 4:Comment on Figure 1: (Category Selection Process Flow)ATC is concerned that the flow chart is assigning a new requirement for CIP-002-2 requirement 1. Based on the proposed flow chart, it seems that an entity has to determine prior to commissioning, any planned changes that would place a facility on an entity's Critical Asset list. We believe that the flow chart should be modified to state that a planned change to a known Critical Asset has to be Compliant upon commissioning and that a planned change which causes an existing facility to be placed on the Critical Asset list be allowed to follow Category 2. This additional clarity would address our concern of pre-determination of a Critical Asset for all planned changes. Would an entity be non-compliant if following a completion of planned change the entity subsequently determines that the facility is a Critical Asset? We are asking this question because the flow chart seems to be indicating that entities have to determine Critical Asset prior to commissioning, and if they determined later that a facility is a Critical Asset that entity could be found non-compliant. ATC suggest the following changes: Clarify that for existing Critical Assets any changes to its associated Critical Cyber Assets shall be compliant upon commissioning. Any newly identified Critical Assets will have to follow Category 2 for its associated Critical Cyber Assets. We believe that this change would accurately align with the existing CIP standards. Comments on the Category X (1, 2 and 3) Scenarios: (Page 6 and 7)The SDT has identified three Scenarios a) Category 1 Scenario, b) Category 2 Scenario, and c) Compliant upon Commissioning. Are these scenarios meant to be examples or does the SDT intend on these being specific scenarios meant to define Figure 1 Item 5: Second paragraph page 10: ("Registered Entities are encouraged when combining separate risk-based"?) ATC believes that the proposed Implementation plan needs to contain a qualifying statement that the annual application of an entities risk-based assessment methodology allows for the addition or removal of Critical Assets. Standard CIP-002 allows an entity to update its list based on the application of the risk-based assessment methodology and does not require a demonstration of "extraordinary circumstances" for removing a previously identified Critical Asset from its list. We believe that this statement is inserting additional compliance obligations that are not contained within the standard. Suggested Modification: Delete the first sentence. If the SDT does not agree with our suggestion, they need to indicate the language contained within CIP-002 which supports the inclusion of phrase "demonstrate extraordinary circumstances" within the standard. Item 6:Table 1: ATC does not believe that enough clarity exists between the phrase Existing Asset and Planned modification. Is a company non-compliance with CIP-002 if a planned modification becomes a Critical Asset following commissioning? (Example: An upgrade is made to an existing asset and it was not identified previously as a Critical Asset. Following commissioning: During the annual application of an entity's

Organization	Yes or No	Question 4 Comment
		risk-based assessment methodology the new asset is identified as a Critical Asset. Does category 2 apply?) Item 7:Table 2: ATC does not believe that 12 months is sufficient enough time for an entity to become compliant with all of the CIP standards. (CIP-003 - CIP-009) We believe that an 18 month window is needed for all Category 2 milestones. In addition, ATC believes that all of the standards should have the same milestone completion date. Although we agree that some Requirements can be done earlier we believe that having the same milestone window gives the entity the ability to put in place a more comprehensive implementation plan that aligns with bringing the Critical Asset into compliance. We don't believe that this reduces security but makes the implementation plan easier to manage and implement. The proposed timelines are problematic. If the electronic security perimeter and physical security need to be in place in 12 months, why is the training allowed to take 18 months? The training should be complete prior to implementing the changes. The varying timeline requirements add to the complexity of Milestone Category 2, which further supports making them all the same. Item 7a:Lastly, ATC believe that the SDT needs to move from a "month" counter to a "day" counter in Table 2. ATC is making this suggestion because an entity would be penalized with fewer days because its milestone month includes February. If the SDT disagrees with our suggestion, then we ask that they specify how many days are in a "month" and when does an entity start counting "months". When does the month counter start? Examples: An entity identifies a Critical Asset on the 1st day of a month. Does the counter start in the next month or does the month in which it was identified count? June 1st and entity identifies a new Critical Asset What is the milestone date for CIP-003 R4, R5 and R6? These requirements currently give an entity 6 months to reach compliance. A) December 31st or B) November 30th Would you give a different answer if the identification happens on June 30th? Additional information: FERC Docket RD09-7 states that the quarter in which something takes place is counted as part of the effective day counter. (See Footnote 8) In other words, FERC sees no difference between the June 1st and June 30th date, but in reality, compliance is either given an additional 30 days (June 1st) or loses 30 days (June 30th). ATC believes that this can be avoided if the team uses a day counter. (Calendar Days)

Response:

Item 1: The term Compliant is defined in the Version 1 Implementation Plan. This definition will be included in the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities.

Item 2: Newly Registered Entity Scenario 1 (Application of Category 3 deals with "A Merger of Two or More Registered Entities where Two or More of the Predecessor Registered Entities has Identified at Least One Critical Cyber Asset", and does not address cases where new cyber assets are

Organization	Yes or No	Question 4 Comment
commissioned in an existing Critical Asset. The Standards Drafting Team assumes you mean Newly Registered Entity Scenario 1 (Application of Category 3 and has added additional clarification in the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities. **Item 3: This could apply to Category 1 or 2 scenarios. Additional clarification has been included in the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities.** **Item 4: The flow chart is a simplified flow for illustration and is not intended to cover all possible scenarios. A more detailed description of the Categories follows the flow chart. It is the opinion of the SDT that the combination of the flow chart, the detailed descriptions and the scenarios present an accurate and comprehensive treatment of the application of the categories and the implementation tables.** **Item 5: It is the opinion of the SDT that the current language does not imply a requirement, but that Responsible Entities are "encouraged" to ensure that no Critical Asset or Critical Cyber Asset has been dropped as a result of the combination of the risk-based methodologies, and the inclusion of the "extraordinary circumstances" applies to assets dropped as a result of the combination, as clearly stated in the paragraph, and not as a result of the normal annual application of the same methodology. It is the opinion of the SDT that if assets are dropped as a result of a combination of risk-based methodologies, Responsible Entities should be "encouraged" to look into the circumstances that caused these drops.** **Item 6: It is the opinion of the SDT that the Implementation Plan, when considered in totality, is clear on a newly identified Critical Asset. Category 1 or Category 2 applies depending on whether the Responsible Entity has an existing CIP Program covering existing Critical Cyber Assets or not.** **Item 7: The Category 2 milestones have been simplified by using 6 month increments. It is the opinion of the SDT that the 6 month increments reflects adequately the graduated complexity of the requirements. In reference to the question about the 12 months for the implementation of electronic security perimeters and physical security perimeters, it is the opinion of the SDT that 6 months provides enough time for entities to complete the training of the personnel identified as a result of the implementation of the electronic and physical security perimeters.** **Item 7a: It is the opinion of the SDT that the month counter begins the first day of the month following a triggering event.**		
MidAmerican Energy Company	Yes	Implementation plan for Newly Identified Critical Cyber Assets: MidAmerican appreciates the specificity in the implementation plan for newly identified Critical Cyber Assets, identified under table 2. Four paragraphs (periodicity or recurrence of the requirement activity, prescribed record retention periods, specific event triggered requirements and records to demonstrate compliance when there is no specified periodicity) provide clarification. Newly Registered Entity Scenarios, Scenario 3a: When combining separate risk-based methodologies, a methodology that provides the most robust level of protection against a cyber attack should be selected. The resulting methodology should be applied to the combined system with no requirement that the resultant list contain all of the critical assets previously identified by the two separate methodologies.

Organization	Yes or No	Question 4 Comment
Response: Newly Registered Entity Scenarios, Scenario 3a: It is the opinion of the SDT that the current language does not imply a requirement, but that Responsible Entities are "encouraged" to ensure that no Critical Asset or Critical Cyber Asset has been dropped as a result of the combination of the risk-based methodologies, and the inclusion of the "extraordinary circumstances" applies to assets dropped as a result of the combination, as clearly stated in the paragraph, and not as a result of the normal annual application of the same methodology. It is the opinion of the SDT that if assets are dropped as a result of a combination of riskbased methodologies, Responsible Entities should be "encouraged" to look into the circumstances that caused these drops.		
Consolidated Edison Company of New York INC.	Yes	In the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities document, Page 2, the following paragraph? A number of the NERC Reliability Standard requirements include a prescribed periodicity or recurrence of the requirement activity (e.g., an annual review of documentation). In those instances, the first occurrence of the recurring requirement must be completed by the Compliant milestone date in Table 2. The entity is then required to collect and maintain required "data," "documents," "documentation," "logs," and "records" to demonstrate compliance with the recurring requirement after the Compliant milestone date has been reached.? Should be deleted for the following reasons: It implies a demonstration of compliance prior to the Compliant date: 1. In requirements where a certain action is required to be completed within a period (e.g. "at least annually"), an entity understand that the Responsible Entity is compliant with the requirement if it can produce demonstration of completion of any instance of the action within the period starting at the Compliant date up to the end of the period (a year in the example) and within each subsequent period following that date (in the example, within a year). Entities should not be required to demonstrate compliance through logs and records of the action prior to the Compliant date. Examples in Versions 2 and 3 include CIP-005-2/3 R4, CIP-007-2/3 R8: the required records demonstrating performance of the vulnerability assessment at least annually.CIP-008-2/3 R1.6: the required records demonstrating the annual exercise of the incident response plan.CIP-009-2/3 R2, R5: the required records demonstrating the performance of the tests. 2. For requirements that require periodic reviews of required documentation, there is a separate requirement to document some complying action: a signed and dated document provides the demonstration of compliance to the documentation requirement at or prior to the Compliant date. The separate requirement for periodic (annual in the example) review of the document applies to any review completed at the earlier of any time within the period (a year in the example) from the date of the document creation and the year after the Compliant date, and to any review at any time within each subsequent period (a year in the example) from the last review date thereafter. Entities should not be required to produce records of requirements which specify periodicity prior to the

Organization	Yes or No	Question 4 Comment
		compliant date. If the basis for the periodicity are documents and records which are required through a specific requirement, entities should be required to demonstrate compliance for these documents and records at Compliant date, and should only be required to produce records and logs of the first periodic requirement after the Compliant date. It is outside of the scope of the SAR. In its Order, the FERC's directive with respect to this referenced Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities: We direct NERC to submit, within 90 days of the date of issuance of this order, a compliance filing that includes a revised Version 2 Implementation Plan, addressing the Version 2 CIP Reliability Standards, that clarifies the matters specified in the attachment to this order. This specific issue does not appear as an issue raised by the Order, either in the body of the Order, or in its Attachment listing issues with this Implementation Plan. In addition, it is not an issue addressed in the original corresponding V2 Implementation plan.
Response: Thank you for your comment. The Standards Drafting Team has considered comments on this issue and has determined that this is a compliance issue that is inappropriately addressed in this Implementation Plan. The paragraph will be revised in the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities in the next posting. **The SDT acknowledges that the initial performance date of tasks being performed as part of meeting recurring requirements is problematic from an audit perspective. The SDT also acknowledges that this issue is not confined to the CIP standards alone and hence the impact of this comment (by its nature) goes beyond the scope of this SDT. The NERC Compliance Staff is expected to issue a compliance bulletin addressing this issue.**		
Hydro-Québec TransEnergie (HQT) Independent Electricity System Operator Northeast Power Coordinating Council	Yes	In the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities document, Page 2, the following paragraph: "A number of the NERC Reliability Standard requirements include a prescribed periodicity or recurrence of the requirement activity (e.g., an annual review of documentation). In those instances, the first occurrence of the recurring requirement must be completed by the Compliant milestone date in Table 2. The entity is then required to collect and maintain required "data," "documents," "documentation," "logs," and "records" to demonstrate compliance with the recurring requirement after the Compliant milestone date has been reached. should be deleted for the following reasons: It implies a demonstration of compliance prior to the Compliant date: 1. In requirements where a certain action is required to be completed within a period (e.g. "at least annually"), an entity understands that the Responsible Entity is compliant with the requirement if it can demonstrably produce completion of any instance of the action within the period starting at the Compliant date up to the end of the period (a year in the example), and within each subsequent period following that date (in the example, within a year). Entities should not be required to demonstrate compliance through logs and records of the action prior to the Compliant date. Examples in Versions 2 and 3 include CIP-005-2/3 R4, CIP-007-2/3 R8: the required records demonstrating performance of the vulnerability assessment at least annually.CIP-008-2/3

Organization	Yes or No	Question 4 Comment
		R1.6: the required records demonstrating the annual exercise of the incident response plan.CIP-009-2/3 R2, R5: the required records demonstrating the performance of the tests. 2. For requirements that require periodic reviews of required documentation, there is a separate requirement to document some complying action: a signed and dated document provides the demonstration of compliance to the documentation requirement at or prior to the Compliant date. The separate requirement for periodic (annual in the example) review of the document applies to any review completed at the earlier of any time within the period (a year in the example) from the date of the document creation and the year after the Compliant date, and to any review at any time within each subsequent period (a year in the example) from the last review date thereafter. Entities should not be required to produce records of requirements which specify periodicity prior to the compliant date. If the basis for the periodicity are documents and records which are required through a specific requirement, entities should be required to demonstrate compliance for these documents and records at the Compliant date, and should only be required to produce records and logs of the first periodic requirement after the Compliant date. It is outside of the scope of the SAR. In its Order, the FERC's directive with respect to this referenced Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities: "We direct NERC to submit, within 90 days of the date of issuance of this order, a compliance filing that includes a revised Version 2 Implementation Plan, addressing the Version 2 CIP Reliability Standards, that clarifies the matters specified in the attachment to this order."This specific issue does not appear as an issue raised by the Order, either in the body of the Order, or in its Attachment listing issues with this Implementation Plan. In addition, it is not an issue addressed in the original corresponding V2 Implementation plan.
Response: Thank you for your comment. The Standards Drafting Team has considered comments on this issue and has determined that this is a compliance issue that is inappropriately addressed in this Implementation Plan. The paragraph will be revised in the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities in the next posting. **The SDT acknowledges that the initial performance date of tasks being performed as part of meeting recurring requirements is problematic from an audit perspective. The SDT also acknowledges that this issue is not confined to the CIP standards alone and hence the impact of this comment (by its nature) goes beyond the scope of this SDT. The NERC Compliance Staff is expected to issue a compliance bulletin addressing this issue.**		
Orange and Rockland Utilities Inc	Yes	In the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities document, Page 2, the following paragraph states: A number of the NERC Reliability Standard requirements include a prescribed periodicity or recurrence of the requirement activity (e.g., an annual review of documentation). In those instances, the first occurrence of the recurring requirement must be completed by the Compliant milestone date in Table 2. The entity is then required to collect and maintain required "data," "documents," "documentation," "logs," and "records" to

Organization	Yes or No	Question 4 Comment
		demonstrate compliance with the recurring requirement after the Compliant milestone date has been reached. This statement should be deleted for the following reasons: It implies a demonstration of compliance prior to the Compliant date: 1. In requirements where a certain action is required to be completed within a period (e.g. “at least annually”), an entity understand that the Responsible Entity is compliant with the requirement if it can produce demonstration of completion of any instance of the action within the period starting at the Compliant date up to the end of the period (a year in the example) and within each subsequent period following that date (in the example, within a year). Entities should not be required to demonstrate compliance through logs and records of the action prior to the Compliant date. Examples in Versions 2 and 3 include CIP-005-2/3 R4, CIP-007-2/3 R8: the required records demonstrating performance of the vulnerability assessment at least annually.CIP-008-2/3 R1.6: the required records demonstrating the annual exercise of the incident response plan.CIP-009-2/3 R2, R5: the required records demonstrating the performance of the tests. 2. For requirements that require periodic reviews of required documentation, there is a separate requirement to document some complying action: a signed and dated document provides the demonstration of compliance to the documentation requirement at or prior to the Compliant date. The separate requirement for periodic (annual in the example) review of the document applies to any review completed at the earlier of any time within the period (a year in the example) from the date of the document creation and the year after the Compliant date, and to any review at any time within each subsequent period (a year in the example) from the last review date thereafter. Entities should not be required to produce records of requirements which specify periodicity prior to the compliant date. If the basis for the periodicity are documents and records which are required through a specific requirement, entities should be required to demonstrate compliance for these documents and records at Compliant date, and should only be required to produce records and logs of the first periodic requirement after the Compliant date.? It is outside of the scope of the SAR. In its Order, the FERC’s directive with respect to this referenced Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities: We direct NERC to submit, within 90 days of the date of issuance of this order, a compliance filing that includes a revised Version 2 Implementation Plan, addressing the Version 2 CIP Reliability Standards, that clarifies the matters specified in the attachment to this order. This specific issue does not appear as an issue raised by the Order, either in the body of the Order, or in its Attachment listing issues with this Implementation Plan. In addition, it is not an issue addressed in the original corresponding V2 Implementation plan.
Response: Thank you for your comment. The Standards Drafting Team has considered comments on this issue and has determined that this is a compliance issue that is inappropriately addressed in this Implementation Plan. The paragraph will be revised in the Implementation Plan for Newly		

Organization	Yes or No	Question 4 Comment
Identified Critical Cyber Assets and Newly Registered Entities in the next posting. **The SDT acknowledges that the initial performance date of tasks being performed as part of meeting recurring requirements is problematic from an audit perspective. The SDT also acknowledges that this issue is not confined to the CIP standards alone and hence the impact of this comment (by its nature) goes beyond the scope of this SDT. The NERC Compliance Staff is expected to issue a compliance bulletin addressing this issue.**		
E.ON U.S. LLC	Yes	Modify requirement R1.6.1 to read as follows: R1.6.1 Visitor logs. Utilizing less prescriptive language in this requirement will provide Responsible Entities with the flexibility to reasonably apply the standard to each of the various circumstances that exist in the industry. For example, providing continuous escorts for parties that don't have unrestricted access to the critical cyber equipment or facilities requires additional staffing. Due to, for example, the number of potential contractors that may be "on-site" at any given time, numerous escorts may be required. The use of a "monitor" would not be sufficient because the escort must have enough knowledge to determine if a cyber incident is occurring. E.ON U.S. favors a process whereby contractors procure critical access certification from NERC or the RRO.
Response: The modification suggested by E.ON U.S. does not adequately meet the FERC directive "to develop a modification to Reliability Standard CIP-006-2 … to add a requirement of a visitor control program, including the use of visitor logs to document entry and exit…"		
Progress Energy	Yes	Progress Energy intends to vote Negative in the upcoming ballot primarily because it disagrees with the proposed language in CIP-006-3a, R1.6.1. Specifically, Progress does not agree with the requirement to document the visitor's time and date of exit from Physical Security Perimeters. Progress is aware of the FERC order issued September 30, 2009 which requires logging of entry and exit dates and times for escorted visitors. Nevertheless, as a practical matter, for facilities with multiple PSPs such as large power plants, it is not feasible to maintain visitor logs for egress when frequent daily or hourly entries to/exits from such PSPs occur, such as during an outage. More importantly, Progress believes that the value of an authorized escort is to maintain continuous surveillance, accountability, and control over the visitor whenever the visitor is within the PSP. Requiring the logging of egress dates and times for escorted visitors does not provide any additional CIP benefit because it does not improve the security of the PSP in real time. It would, however, greatly increase cost, reduce productivity, and create opportunity for inadvertent violation of the NERC requirement. FERC did not order that personnel with unescorted access also be required to log egress times and dates, presumably because there is no benefit to doing so. Likewise, if the escort is properly performing his/her function, there would be no reason to log egress times and dates for those being escorted.
Response: The SDT does not agree that the requirement to log the ingress and egress of visitors from Physical Security Perimeters greatly increases costs and reduces productivity. It is the opinion of the SDT that documenting precisely when unauthorized individuals had escorted access inside Physical Security Perimeters is a key element of an acceptable visitor control program. Outages due to emergencies may be addressed by CIP-003 R1 (Policy), and in CIP-004 R2 and R3 (Training and Personnel Risk Assessment). The SDT reminds the entity that it also has the discretion to grant an		

Organization	Yes or No	Question 4 Comment
individual authorized unescorted physical access to the Physical Security Perimeter should the requirement of escorting and logging ingress and egress prove burdensome.		
NextEra Energy Resources Silvia Parada-Mitchell Florida Power & Light	Yes	Regarding CIP-006-3a, R1.6.1 specifically, we do not agree with the requirement to document the visitor's time and date of exit from Physical Security Perimeters. Facilities with multiple PSPs such as large power plants, it is not feasible to maintain visitor logs for egress when frequent daily or hourly entries to/exits from such PSPs occur, such as during an outage. We believe the value of an authorized escort is to maintain continuous surveillance, accountability, and control over the visitor whenever the visitor is within the PSP. Requiring the logging of egress dates and times for escorted visitors does not provide any additional CIP benefit because it does not improve the security of the PSP in real time. It would, however, greatly increase cost, reduce productivity, and create opportunity for inadvertent violation of the NERC requirement.
Response: The SDT does not agree that the requirement to log the ingress and egress of visitors from Physical Security Perimeters greatly increases costs and reduces productivity. It is the opinion of the SDT that documenting precisely when unauthorized individuals had escorted access inside Physical Security Perimeters is a key element of an acceptable visitor control program. Outages due to emergencies maybe addressed by CIP-003 R1 (Policy), and in CIP-004 R2 and R3 (Training and Personnel Risk Assessment). The SDT reminds the entity that it also has the discretion to grant an individual authorized unescorted physical access to the Physical Security Perimeter should the requirement of escorting and logging ingress and egress prove burdensome.		
PacifiCorp	Yes	Regarding the implementation plan treatment of merging Responsibilities Entities: when combining separate risk-based methodologies, PacifiCorp believes that each separate methodology should be applied to the combined system and the methodology that provides the most robust level of protection against a cyber attack based on the critical assets identified should be selected. The selected methodology should be applied to the combined system with no requirement that the resultant list contain all of the critical assets previously identified by the two separate methodologies.
Response: It is the opinion of the SDT that the current language does not imply a requirement, but that Responsible Entities are "encouraged" to ensure that no Critical Asset or Critical Cyber Asset has been dropped as a result of the combination of the risk-based methodologies, and the inclusion of the "extraordinary circumstances" applies to assets dropped as a result of the combination, as clearly stated in the paragraph, and not as a result of the normal annual application of the same methodology. It is the opinion of the SDT that if assets are dropped as a result of a combination of risk-based methodologies, Responsible Entities should be "encouraged" to look into the circumstances that caused these drops.		
Portland General Electric Company	Yes	The Draft Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities contains the following statement: "A number of the NERC Reliability Standard requirements include a prescribed periodicity or recurrence of the requirement activity (e.g., an annual review of documentation). In those instances, the first occurrence of the recurring requirement must be completed by the Compliant milestone date in Table 2." PGE strongly disagrees with this approach. PGE believes that this language

Organization	Yes or No	Question 4 Comment
		directly contradicts the plain language understanding of an "annual" requirement, and this is made clear by reference to the Standards currently under consideration. Looking at Standard CIP-003-3 R4 (Information Protection), for example, a Responsible Entity "shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets." It is clear, then, that a Registered Entity must have in place an Information Protection Program on or before the "Compliant" milestone date. However, R4.3 of this Standard provides that the Responsible Entity "shall, at least annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment." (Emphasis added.) This R4.3 clearly contemplates an "assessment" of the information protection program that takes place after the initial implementation of that program and recurs "annually" thereafter. Applying the interpretation of "annual" set forth in the Draft Implementation Plan to this Standard, an entity would have to "implement and document" a program, and also "assess adherence" to that same program by the "Compliant" milestone date. Determining adherence to a new program requires that the program be in place and exercised for a period of time, otherwise you do not have enough relevant data to "assess adherence". Similarly, in Standard CIP-007-3 R8 (Cyber Vulnerability Assessment), a Responsible Entity "shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually." Looking at the sub requirements within this R8, it is clear that this "annual" review requirement is triggered after the "Compliant" milestone date. Requirement 8.2, for example, requires the entity to "verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled." This requirement pertaining to ports and services is set forth separately in R2 of the same Standard. As such, the plain language interpretation of this Standard is that an entity must establish compliance with the stand-alone R2 requirement pertaining to ports and services on or before the "Compliant" milestone date, and then perform a Cyber Vulnerability Assessment annually thereafter to test ongoing compliance. If the Cyber Vulnerability Assessment (R8) must be performed for the first time on or before the "Compliant" milestone date, then it is duplicative of other requirements within the Standard. It is clear, then, that a requirement to perform an action on an annual basis gives the entity a year from the time that the requirement reaches the Compliant milestone date for the first instance of performing that action. The Standard Drafting Team's approach would require a utility to comply with the requirement before the Compliant milestone date, rendering the Compliant milestone date meaningless. An entity has not failed to meet the requirement until it fails to complete the requirement activity on an annual basis. By definition this cannot take place until two conditions have been met: (1) the requirement has been mandatory on the entity (i.e., at the Compliant stage); and (2) the entity has failed to perform the requirement activity at least as often as once a year. The entity's failure to perform the activity prior to expiration of the "annual" period following the Compliant milestone cannot constitute noncompliance because the activity can still be taking place on an annual basis. Construing all requirements with a prescribed periodicity to require the first performance of the requirement activity prior to the Compliant milestone can undermine the intent of the standard, which is for the registered entity to perform the activity in keeping with their typical annual performance cycles. For example,

Organization	Yes or No	Question 4 Comment
		a requirement that reaches the "Compliant" milestone on January 1 can include an annual performance activity that the entity typically does as part of an outage drill which is done every September. The entity should not be forced to alter their typical annual schedule in order to meet the requirement before it has reached the "Compliant" stage. This approach is not supported by past standard development activity or by FERC Order and represents a fundamental shift in NERC's approach to such requirements with prescribed periodicities. Given that many such requirements are currently or will soon be at the Compliant milestone date, such a shift in approach would require adequate notice to the affected entities.
Response: Thank you for your comment. The Standards Drafting Team has considered comments on this issue and has determined that this is a compliance issue that is inappropriately addressed in this Implementation Plan. The paragraph will be revised in the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities in the next posting. **The SDT acknowledges that the initial performance date of tasks being performed as part of meeting recurring requirements is problematic from an audit perspective. The SDT also acknowledges that this issue is not confined to the CIP standards alone and hence the impact of this comment (by its nature) goes beyond the scope of this SDT. The NERC Compliance Staff is expected to issue a compliance bulletin addressing this issue.**		
Manitoba Hydro	Yes	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

Organization	Yes or No	Question 4 Comment
		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. The Standards Drafting Team has considered comments on this issue and has determined that this is a compliance issue that is inappropriately addressed in this Implementation Plan. The paragraph will be revised in the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities in the next posting. **The SDT acknowledges that the initial performance date of tasks being performed as part of meeting recurring requirements is problematic from an audit perspective. The SDT also acknowledges that this issue is not confined to the CIP standards alone and hence the impact of this comment (by its nature) goes beyond the scope of this SDT. The NERC Compliance Staff is expected to issue a compliance bulletin addressing this issue.**		
Dominion Virginia Power	Yes	The proposed requirement CIP-006-3a R1.6.1 is redundant to and/or conflicts with requirement R6. A suggested modification: R1.6 Each PSP shall be governed by a visitor control program which, at a minimum, provides the following requirements: R1.6.1 Continuous escorting of any personnel without authorized unescorted access to the PSP R1.6.2 Meets the logging requirements found in CIP-006-3a R6. If the above change is not considered, please amend CIP-006-3a R6 to indicate that it only applies to non-visitors.
Response: The SDT clarifies that Requirement CIP-006 R1.6 specifies a visitor control program. Under this requirement, the “visitor’s identity, time and date of entry to and exit from Physical Security Perimeters” must be logged. The SDT did not modify the requirements for individuals with authorized unescorted access to the Physical Security Perimeter. CIP-006 R6 requires a log that captures “time of access” for all individuals who enter a Physical Security Perimeter. Project 2008-15 “Interpretation of CIP-006-1a By US Army Corps of Engineers” clarifies that the term “time of access” indeed refers to the time an authorized individual enters the physical security perimeter.		
Silicon Valley Power	Yes	Violation Severity Levels in some cases do not provide for either Moderate or Low levels in all cases
Response: Not all requirements have four violation severity levels. Note that the impact to reliability of a requirement is measured by the VRF; the VSL is an indication of the lack of compliance with the requirement.		
Midwest ISO Standards Collaborators	Yes	We agree that the modifications to the standards and implementation plans meet the intent of the FERC directives but do have some suggestions for improving them. 1) In the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities

Organization	Yes or No	Question 4 Comment
		document, Category 1 Scenario under Newly Registered Entity Scenarios on page 8 appears to address what is largely a registration issue. It appears that the document assumes that the merging entities will join their registration but this may not be the case. There is no NERC rule that requires two utilities that operate separate balancing authorities to merge those balancing authorities once the merger is completed. They may continue to be registered as two BAs as a result. Consider the Duke-Cinergy merger as example of when this happened. The scenario should be updated to consider these issues or to identify the assumptions made. Further, we suggest the that the last two sentences in the second paragraph under the Category 1 Scenario beginning with following language should be deleted as a result: "it would be preferred that a single program be the result of this analysis, however,". 2) In the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities document, the first sentence (as shown below) in the second paragraph in section (a) under the Category 3 Scenario under Newly Registered Entity Scenarios should be deleted. That sentence is: "Registered Entities are encouraged when combining separate risk-based Critical Asset identification methodologies to ensure that, absent extraordinary circumstances, the resulting methodology produces a resultant list of Critical Assets that contains at least the same Critical Assets as were identified by all the predecessor Registered Entity's risk-based Critical Asset identification methodologies, as well as at least the same list of Critical Cyber Assets associated with the Critical Assets." This sentence assumes that the primary purpose of the CIP standards is to protect the Critical Cyber Assets and that once a Critical Cyber Asset always a Critical Cyber Asset. Rather, the purpose is to protect the grid by ensuring it can't be compromised by hacking of a cyber asset. It demonstrates ignorance that how the grid is operated can, will and should affect the Critical Asset list. Mergers can affect how the grid is operated and ultimately the Critical Asset list. As an example, a merged utility may combine its two previously separate Balancing Authorities into a single Balancing Authority. This would cause the Contingency Reserve obligation to increase and could cause a generating unit to be no longer a Critical Asset as a result. Table C-2 in NERC's Security Guideline for the Electricity Sector: Identifying Critical Assets document specifically identifies a unit exceeding the Contingency Reserve obligation as a reason to classify a generating unit as a Critical Asset. This is hardly an extraordinary circumstance. Further, this outcome would occur even if the two merged entities had identical Critical Asset identification methodologies. 3) In an August 10, 2009 informational filing to FERC, NERC laid out a new approach to define one VRF at the requirement level that applies to the requirement and its sub-requirements and applies a single comprehensive set of VSLs to the main requirement that categorizes non-compliance with the main requirement and sub-requirement. This approach should be applied here. 4) The VRFs on CIP-006-3a R1.6 and R1.6.1 should be Lower because it is completely an administrative requirement intended to demonstrate to the Commission that visitors are escorted. Failure to have a visitor control program that includes logs is hardly a risk especially when one considers that other requirements such as CIP-006-3a R4 already mandate that a secure perimeter would be maintained. With R4 in place, a visitor

Organization	Yes or No	Question 4 Comment
		could not gain unnecessary access even if there were no visitor log maintained. 5) For the VSLs on CIP-006-3a R1.6, a potential non-compliance that is likely to occur that is not considered is for the case of not logging egress when ingress is logged. VSLs could be written based on the number of visitors that don't have egress logged. Likely, if ingress is not logged, egress will not be logged and no record of the visitor will exist. For this reason, the Moderate and High VSLs will likely never apply. The Moderate VSL appears to assume that the compliance auditor will be able to review a record of all visitors that were not logged into the visitor log. The visitor log is intended to be the record of visitors so how will the compliance auditor know a visitor wasn't logged. No evidence would exist. 6) We suggest the following wording for CIP-006-3a R1.6.1 would be more succinct and provide the same meaning. "Visitor logs to document the visitor's identity, time and date of entry to and exit from Physical Security Perimeters, and the identity of the escort with authorized unescorted physical access performing the escort." 7) The drafting team should consider defining the term visitors in R1.6 and eliminating the clause in parentheses. Clauses like these could be misconstrued from its intention which is to define visitor. A definition is cleaner and clearer.

Response:

1) **This section makes no assumption that merged companies or organizations automatically result in merged Registered Entities. It describes a situation when two Responsible Entities merge into a single Responsible Entity: "A Merger of Two or More Registered Entities…." (emphasis inserted in this response).**

   Regarding the issue of preference for single program, the Implementation Plan expresses a preference and not a requirement. It is the opinion of the SDT that a single program reduces complexity for both the Responsible Entity and the compliance monitoring and enforcing organizations. Further, it reinforces that "Registered Entity specific circumstances may dictate or allow the two programs to continue separately."

2) **It is the opinion of the SDT that the current language does not imply a requirement, but that Responsible Entities are "encouraged" to ensure that no Critical Asset or Critical Cyber Asset has been dropped as a result of the combination of the risk-based methodologies, and the inclusion of the "extraordinary circumstances" applies to assets dropped as a result of the combination, as clearly stated in the paragraph, and not as a result of the normal annual application of the same methodology. It is the opinion of the SDT that if assets are dropped as a result of a combination of risk-based methodologies, Responsible Entities should be "encouraged" to look into the circumstances that caused these drops.**

3) **The VSLs developed for the Version 3 standards are consistent with other VSLs for the existing Version 2 CIP Standards. The SDT will consider using the new VSL methodology in the next version of the standards.**

4) **It is the opinion of the SDT that facilities security is critically important, as also indicated by the Commission, and that visitor control programs and visitor logs are an essential element of sound facilities security. Therefore, it is the opinion of the SDT that a VRF of "Medium" is appropriate for**

Organization	Yes or No	Question 4 Comment
		R1.6 and R1.6.1. **5) The case of not logging egress when ingress is logged is considered under the Lower VSL as written. The SDT agrees that the cases of Moderate and High VSLs may be difficult to identify as a finding during an audit, but are in fact likely scenarios that may be self-reported by the entity. In addition, while the visitor log is the record of visitors, there may be other records available such as video recordings of a PSP that may show that a visitor entered without completing the required log information.** **6) The Commission discussed elements of a common visitor log as highlighted in the comment. However, the Commission directive only specified the use of visitor logs to document entry and exit. The standard drafting team has made the modifications to be consistent with the FERC directive.** **The elements of the visitor log selected by the SDT represent a baseline for an acceptable visitor log and entities are free to exercise their flexibility in implementing a more rigorous visitor log if they so choose.** **7) The SDT agrees that definitions in the NERC glossary provide clean and clear information to the entity. However, definitions in the glossary must also apply across all NERC standards and thus often have unintended consequences. In the case of the definition of visitors, it is the opinion of the SDT that the parenthetical definition is clear enough to not be misconstrued from its intention.**
Duke Energy	Yes	We support the MISO Standards Collaborators' comments, and have the following additional comments: 1. NERC: V3 Implementation Plan: The Responsible Entities shall be compliant with all requirements on the Effective Date specified in each standard. Can the industry have some kind of an estimate as to when that will be 2. Implementation Plan for Newly Identified Critical Assets. Comment/question to NERC. Utilities really want to do the right thing. It is quite possible that new Critical Assets may be identified late in 2009. CIP version 1 has no implementation plan for such new identified Critical Assets, and NERC acknowledges this “compliance gap”. An implementation plan to address this gap is being proposed here. This same implementation plan was proposed in v2. A compliance gap exists for newly identified CA until this proposed effective date. This implementation plan for newly identified Critical assets is desperately needed by the utility. The implementation plan was poorly written when submitted by NERC to FERC and was, therefore, not included in the FERC approved Version 2 materials. This is no fault of the utilities. What is the proposed effective date of the Implementation Plan for Newly Identified Critical Assets? If a utility has newly identified Critical Assets between the compliance date for CIP version 1 and the effective date of the Implementation Plan for Newly Identified Assets, what schedule should they follow for the implementation of CIP? It is not reasonable to expect that newly identified Critical Assets are immediately “auditably compliant” under CIP version 1. What remedy is available to the utilities short of non-compliance related to newly identified Critical Assets prior to the effective date of this Implementation Plan? 3. Version 1 Implementation Plan Retirement: The Version 1 Implementation Plan will be retired once all

Organization	Yes or No	Question 4 Comment
		Entities in Tables 1, 2, and 3 of that plan have achieved their Compliant state. ”The wording in the NERC material states that Version 1 Implementation Plan will not be retired until the Entities achieve compliant state. Is this true” Shouldn’t the posting read “Version 1 Implementation Plan will be retired once the target dates explained in the Phased In Plan expire”? 4. Dropping “Auditably Compliant”. The term “auditably compliant” has been dropped from this future version of the implementation plan. We do not object, but we have a clarifying question: Auditably compliant referred to the need to have 12 months of data. At what point is the utility expected to have 12 months of data accumulated for review during an audit? Is it at the compliant stage or 12 months subsequent to compliant stage?

Response:

1) **NERC has no control over when various milestones in the regulatory approval process can be achieved. The effective date formula is based on the date of regulatory approval.**
2) **FERC approved the Implementation Plan for Newly Identified Critical Cyber Assets in its order approving the Version 2 CIP Standards. These are effective April 1st, 2010. The SDT acknowledges there is a compliance gap, and in the period after an entity's compliance date and extending to April 1, 2010, this issue should be addressed through the Compliance Monitoring and Enforcement Program.**
3) **The wording in the “Implementation Plan for Version 3 of Cyber Security Standards CIP-002-3 through CIP-009-3” has been clarified.**
4) **This issue is a compliance issue which must be addressed by NERC Compliance. The paragraph in the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities has been removed.**