

## Consideration of Comments on 1st Draft of SAR to Revise Cyber Security Standards — Project 2008-06

The Standards Committee thanks all commenters who submitted comments on the 1st draft of the SAR to revise the Cyber Security standards. These standards were posted for a 30-day public comment period from March 20, 2008 through April 19, 2009. The stakeholders were asked to provide feedback on the SAR through a special Standard Comment Form. There were more than 34 sets of comments, including comments from more than 100 different people from approximately 50 companies representing 8 of the 10 Industry Segments as shown in the table on the following pages.

The 1st draft of the SAR focused on addressing the directives and recommendations contained in the FERC Order 706, and when posted, the drafting team asked stakeholders to identify any other issues encountered while attempting to follow the CIP standards. In response to stakeholder comments, the SAR DT made the following changes to the original SAR:

The SAR DT had proposed expanding the applicability of the existing standards to include requirements for the Regional Entity and the Purchasing-selling Entity. While most commenters agreed with the addition of the Regional Entity, most disagree with the addition of the Purchasing-selling Entity and the SAR was modified to remove the Purchasing-selling Entity as a responsible entity.

Most of the commenters agreed that the scope of the standards action to address the items identified in the FERC Order 706 is appropriate. Some went on to suggest that a list of these items accompany the SAR to which the SAR DT agreed.

There were many comments objecting to the reference to the Functional Model and the possible inclusion of requirements assigned to the "Demand Side Aggregator." Commenters indicated that the Load-serving Entity is already required to comply with the CIP standards, and the Load-serving Entity performs many of the same tasks as those assigned to the Demand Side Aggregator. Based on these comments, the drafting team removed the reference to the Functional Model and the Demand Side Aggregator from the revised SAR.

Some commenters suggested that the SAR be modified to include a specific reference to the Interpretation of CIP-006-1, and the drafting team has done so. As part of the standards process, the interpretation must be incorporated into a standard when it is revised.

Several commenters suggested that the Cyber Security Standard Drafting Team coordinate its work with other Cyber-related standards, guidelines and activities, and the SAR drafting team added the following to the SAR:

- Consider other cyber security related documents such as NIST, ISO 27000 Family, CIPC WG Risk Assessment Guideline, MITRE corporation technical report, DHS, National Laboratories papers, DOE 417, IEC, ISA, etc.
- Stay apprised of coordination work between FERC, NEI and NRC in regard to the Nuclear facility exemption issue with respect to regulatory gaps. As necessary modify the standards to reflect current determinations.

The following issues identified by stakeholders have been added to a list of issues for the standard drafting team to address and appended the list to the SAR as Attachment 3.

### Industry Education

- Consider what to do with the existing FAQ document e.g., modify, replace.

- Consider how to provide additional guidance in support of these standards, e.g., Technical Reference documents, guidelines, white papers.
- Consider development of a guideline document to address extended LANs over multiple geographically dispersed locations.

#### Balloting and Implementation

- Determine the timing and grouping of revisions to be submitted to industry for comment and ballot, e.g., multi-phase or other approach.
- Determine the optimum implementation plan for revised CIP standards in this project.
- Address when newly identified critical assets or critical cyber assets, newly acquired equipment or assets, etc. must come into compliance with CIP standards.
- Address compliance issue where internal requirements exceed NERC requirements. Clarify in view of language contained in FERC Order 706 paragraph 377.

#### Clarify Existing Requirements

- Consider the need for different requirements for different environments e.g., control center, substation and generation plant.
- Clarify how serial and wireless devices are subject to these standards. Refer to pp 278 and 285 of FERC Order 706.

#### Other Issues

- Consider issues surrounding protection of data in motion.
- Consider the issue of hybrid devices that use both serial and routable protocols.
- Consider the issue of data versus information (electronic and/or hardcopy lists, drawings, etc.) protection including transport and transmittal of such information.

In this document comments have been organized so it is easier to interpret the comments. All comments received can be viewed in their original format at the following site:

[http://www.nerc.com/~filez/standards/Project\\_2008-06\\_Cyber\\_Security.html](http://www.nerc.com/~filez/standards/Project_2008-06_Cyber_Security.html)

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](mailto:gerry.adamski@nerc.net). In addition, there is a NERC Reliability Standards Appeals Process.<sup>1</sup>

---

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

**Consideration of Comments on 1st Draft of SAR to Revise Cyber Security Standards  
— Project 2008-06**

**Index to Questions, Comments, and Responses**

1. Do you agree with the scope of the proposed standards action? .....	9
2. This SAR proposes to add the Regional Entities and Purchasing-Selling Entity functions to the applicability section of the revised standards. If additional Functional Model changes are made (or if changes are made to the Compliance Registration Criteria) as a direct result of Order 706 (i.e., Demand Side Aggregator — see Order 706 paragraph 51), which directly impact the applicable functions, conforming modifications will be made to the cyber security standards. Do you agree with these proposed changes to the applicability sections of these standards?.....	18
3. If you are aware of any regional variances or associated business practices that we should consider with this SAR please identify them here. ....	29
4. Do you agree with the “multi-phase” approach identified in the SAR? (The SAR’s proposal is to take the easiest modifications through the posting and balloting cycles first, followed by one or more sets of modifications to address those directives that will take more time.) .....	30
5. Based on the limited experience of implementing the current standards, are there any other issues that are not addressed in Order 706 that should be changed? .....	37
6. If you have any other comments on this SAR that you haven’t already provided in response to the prior six questions, please provide them here.....	49

Consideration of Comments on 1st Draft of SAR to Revise Cyber Security Standards — Project 2008-06

Individual or group.	Name	Organization	RBB Segment																
Individual	Thad Ness	AEP	5 - Electric Generators, 6 - Electricity Brokers, Aggregators , 1 - Transmission Owners, 3 - Load-serving Entities																
Individual	Gerald Freese	American Electric Power	3 - Load-serving Entities, 5 - Electric Generators, 6 - Electricity Brokers, Aggregators , 1 - Transmission Owners																
Individual	Jason Shaver	American Transmission Company	1 - Transmission Owners																
Individual	Paul Kerr	Coral Power, L.L.C.	6 - Electricity Brokers, Aggregators																
Individual	Kent Kujala	Detroit Edison	3 - Load-serving Entities, 5 - Electric Generators, 4 - Transmission-dependent Utilities																
Group	Louis Slade	Dominion Resources Services, Inc.	3 - Load-serving Entities, 6 - Electricity Brokers, Aggregators , 5 - Electric Generators	<table border="1"> <thead> <tr> <th></th> <th>Additional Member</th> <th>Additional Organization</th> <th>Region</th> <th>Segment Selection</th> </tr> </thead> <tbody> <tr> <td>1.</td> <td>Harold Adams</td> <td></td> <td>RFC</td> <td>3, 5, 6</td> </tr> <tr> <td>2.</td> <td>Jalal Babik</td> <td></td> <td>SERC</td> <td>3, 5, 6</td> </tr> </tbody> </table>		Additional Member	Additional Organization	Region	Segment Selection	1.	Harold Adams		RFC	3, 5, 6	2.	Jalal Babik		SERC	3, 5, 6
	Additional Member	Additional Organization	Region	Segment Selection															
1.	Harold Adams		RFC	3, 5, 6															
2.	Jalal Babik		SERC	3, 5, 6															
Individual	Greg Rowland	Duke Energy	1 - Transmission Owners, 3 - Load-serving Entities, 5 - Electric Generators, 6 - Electricity Brokers, Aggregators																
Group	Jack Cashin	Electric Power Supply Association	5 - Electric Generators																
Individual	Denise Roeder	ElectriCities of North Carolina, Inc.	6 - Electricity Brokers, Aggregators , 4 - Transmission-dependent Utilities, 3 - Load-serving																

Consideration of Comments on 1st Draft of SAR to Revise Cyber Security Standards — Project 2008-06

Individual or group.	Name	Organization	RBB Segment					
			Entities					
Group	Sam Ciccone	FirstEnergy Corp.	5 - Electric Generators, 6 - Electricity Brokers, Aggregators, 3 - Load-serving Entities, 1 - Transmission Owners					
Individual	David Kiguel	Hydro One Networks Inc.	3 - Load-serving Entities, 1 - Transmission Owners					
Individual	Ken Welch	LK4 Technology Corporation	Not Applicable					
Group	Jason L. Marshall	Midwest ISO	2 - RTOs and ISOs		<b>Additional Member</b>	<b>Additional Organization</b>	<b>Region</b>	<b>Segment Selection</b>
				1.	Joe Knight	Great River Energy	MRO	1
				2.	Kirit Shah	Ameren	SERC	1
				3.	Joeseeph DePoorter	Madison Gas and Electric Company	MRO	3, 4, 5, 6
Individual	Martin R. Hopper	M-S-R Public Power Agency	9 - Federal, State, Provincial Regulatory, or other Government Entities					
Group	Keith Stouffer	National Institute of Standards and Technology	9 - Federal, State, Provincial Regulatory, or other Government Entities		<b>Additional Member</b>	<b>Additional Organization</b>	<b>Region</b>	<b>Segment Selection</b>
				1.	Stu Katzke	NIST	NA - Not Applicable	9
				2.	Marshall Abrams	Mitre	NA - Not Applicable	NA
Group	Lee Pedowicz	NPCC	10 - Regional Reliability Organizations/Regional Entities		<b>Additional Member</b>	<b>Additional Organization</b>	<b>Region</b>	<b>Segment Selection</b>
				1.	Guy Zito	NPCC	NPCC	10
				2.	Brian Hogue	NPCC	NPCC	10

Consideration of Comments on 1st Draft of SAR to Revise Cyber Security Standards — Project 2008-06

Individual or group.	Name	Organization	RBB Segment					
				3.	David Kiguel	Hydro One	NPCC	1, 3
				4.	Kathleen Goodman	ISO New England	NPCC	2
				5.	Ben Li	Independent Electricity System Operator	NPCC	2
Individual	George W. Brady	Ohio Valley Electric Corporation	1 - Transmission Owners					
Individual	Greg Ward / Steve Martin	Oncor Electric Delivery Company LLC	1 - Transmission Owners					
Individual	Ron Falsetti	Ontario IESO	2 - RTOs and ISOs					
Group	Colin Anderson	Ontario Power Generation	5 - Electric Generators					
Group	Robert Mathews	Pacific Gas and Electric Company	1 - Transmission Owners		<b>Additional Member</b>	<b>Additional Organization</b>	<b>Region</b>	<b>Segment Selection</b>
				1.	Dave Ambrose	WAPA - Loveland	WECC	1, 3
				2.	Vern Kissner	Tacoma Power	WECC	
				3.	Marc DeNarie	WAPA - Folsom	WECC	1, 3
				4.	Jeff Mantong	WAPA - Folsom	WECC	1, 3
				5.	Gray Wright	Sierra Pacific Power	WECC	1, 3, 5
				6.	Jamey Sample	CAISO	WECC	2
Individual	Todd Thompson	PJM Interconection	2 - RTOs and ISOs					
Group	Annette Bannon	PPL Generation, LLC	5 - Electric Generators, 6 - Electricity Brokers, Aggregators		<b>Additional Member</b>	<b>Additional Organization</b>	<b>Region</b>	<b>Segment Selection</b>

Consideration of Comments on 1st Draft of SAR to Revise Cyber Security Standards — Project 2008-06

Individual or group.	Name	Organization	RBB Segment						
				1.	Mark Heimbach	PPL EnergyPlus	RFC	6	
				2.	Mark Heimbach	PPL EnergyPlus	MRO	6	
				3.	Mark Heimbach	PPL EnergyPlus	NPCC	6	
				4.	Mark Heimbach	PPL EnergyPlus	SERC	6	
				5.	Mark Heimbach	PPL EnergyPlus	SPP	6	
				6.	Jim Batug	PPL Generation	RFC	5	
				7.	Jim Batug	PPL	NPCC	5	
Group	Phil Riley	Public Service Commission of South Carolina	9 - Federal, State, Provincial Regulatory, or other Government Entities						
Individual	Daniel Hecht	Sempra Energy Trading LLC and Sempra Energy Solutions LLC	6 - Electricity Brokers, Aggregators						
Group	Jim Busbi	Southern Company Services, Inc.	1 - Transmission Owners	<b>Additional Member</b>	<b>Additional Organization</b>	<b>Region</b>	<b>Segment Selection</b>		
				1.	J. T. Wood	Southern Company Services, Inc.	SERC		1
				2.	Roman Carter	Southern Company Services, Inc.	SERC		1
				3.	Marc Butts	Southern Company	SERC		1

Consideration of Comments on 1st Draft of SAR to Revise Cyber Security Standards — Project 2008-06

Individual or group.	Name	Organization	RBB Segment						
						Services, Inc.			
				4.	Jay Cribb	Southern Company Services, Inc.	SERC		1
				5.	Valerie Piazza	Southern Company Services, Inc.	SERC		1
Group	Charles Yeung	Southwest Power Pool	2 - RTOs and ISOs						
Individual	Eric Olson	Transmission Agency of Northern California	1 - Transmission Owners						
Individual	Michael Puscas	United Illuminating	1 - Transmission Owners, 3 - Load-serving Entities						
Individual	William Lucas	We Energies	3 - Load-serving Entities, 5 - Electric Generators						
Group	Robert Mathews - CIIMS Subcommittee Chair	WECC (Steve Rueckert)	10 - Regional Reliability Organizations/Regional Entities						
Group		WECC-NERC PMO - PacifiCorp	1 - Transmission Owners, 3 - Load-serving Entities, 5 - Electric Generators						
Group	Patrick Miller	Western Electricity Coordinating Council	10 - Regional Reliability Organizations/Regional Entities						
Individual	Terri Eaton	Xcel Energy	1 - Transmission Owners, 3 - Load-serving Entities, 5 - Electric Generators, 6 - Electricity Brokers, Aggregators						

## Consideration of Comments on 1st Draft of SAR to Revise Cyber Security Standards — Project 2008-06

### 1. Do you agree with the scope of the proposed standards action?

**Summary Consideration:** Most of the commenters agreed that the scope of the standards action to address the items identified in the FERC Order 706 is appropriate. Some went on to suggest that a list of these items accompany the SAR to which the SAR DT agreed.

There were many comments objecting to the inclusion of Purchasing Selling Entities (PSE) as subject to the CIP-002 through CIP-009 Standards. The SAR DT agreed and removed PSE from the SAR.

In addition, several commenters suggested that the reference to the Functional Model is inappropriate because the Demand-side Aggregator identified in FERC Order 706 performs the same tasks as the Load-serving Entity – and the SAR already identifies the Load-serving Entity as a functional entity with responsibility for some of the requirements in the set of CIP standards. Consequently, the drafting team removed this reference in the revised SAR.

Organization	Question 1:	Question 1 Comments:
Xcel Energy	No	PSEs are involved in scheduling purchase and sales transactions between entities in the wholesale electric market. We are not aware of any <u>activities undertaken by a PSE that could be manipulated from a cyber standpoint and result in compromising the integrity of the bulk electric system</u> . We believe that NERC should be required to provide a credible justification for extending the reach of the CIP standards to PSEs. At this juncture, Xcel Energy does not believe that any such justification has been provided.
<p><b>Response:</b> The NERC CIP Cyber Security Standards are applicable to entities that operate or impact the operation of facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System. The SAR DT believes that the PSE serves more of an economic role, and less of a reliability role, and that while their systems could be compromised the impact of such compromise would not affect the reliability or operability of the Bulk Electric System due to the other reliability operations controls in place. Therefore the PSE is removed from the SAR as an applicable entity.</p>		
American Transmission Company	No	The SAR should be revised to include a list of all FERC issued directives including the identification of any specific due dates. This additional information will help the industry understand the amount of work the standards drafting team is being assigned. NERC likely has this information so the inclusion of the data should be simple.
<p><b>Response:</b> The SAR DT agrees that a list of changes to be made to the CIP standards is appropriate for inclusion in the SAR as a scoping reference. The team disagrees that the intent of the list would be to either estimate the quantity or length of work to be performed or prioritize the work to be undertaken.</p>		
NPCC	No	1. The SAR is not specific on which CIP standards are "low hanging fruit", which ones contain more contentious issues than the others. It does not identify a proposed implementation plan that would support multiple revisions

Consideration of Comments on 1st Draft of SAR to Revise Cyber Security Standards — Project 2008-06

Organization	Question 1:	Question 1 Comments:
		<p>to the standards, whereas some changes would be reviewed by industry, balloted, and submitted for approval.</p> <p>2. The SAR indicates that if additional Functional Model changes are made as a direct result of Order 706 (i.e., Demand Side Aggregator--see Order 706 paragraph 51), which directly impact the applicable functions, these functional entities will be added to the scope of the cyber security standards resulting from this SAR. Our read of Section 51 shows that FERC has not asked NERC to revise its functional model; it merely directed ??that NERC should register demand side aggregators if the loss of their load shedding capability, for reasons such as a cyber incident, would affect the reliability or operability of the Bulk-Power System.? In our view, registering an organization or group to ensure compliance with reliability standards does not require that organization or group to be defined in the functional model as long as the functions they register to perform conform with the tasks listed in the model under an appropriate entity. In this case, we expect the "Demand Side Aggregator", which we believe performs the tasks listed under the LSE in the model, will register as an LSE. Hence, we do not expect the functional model will be revised to address this directive. As a result, we do not agree that this speculative revision to scope statement should be in the SAR.</p> <p>3. The originating cause and this SAR's scope should not be limited to FERC Order 706. Experiences from stakeholder's implementing the Cyber Standards should be taken into consideration as lessons learned as part of the scope for developing Standards. Extending the SAR beyond FERC Order 706 should only be done if it will not affect timelines given by FERC. Also, interpretations made subsequent to the standards should be formally codified into the appropriate places in the standards, such as the CIP-006 interpretation and any FAQ interpretations.</p>
<p><b>Response:</b></p> <ol style="list-style-type: none"> <li>1. The SAR DT agrees that a list of changes to be made to the CIP standards is appropriate for inclusion in the SAR as a scoping reference. It is more appropriate that the SDT determine the timing and grouping of revisions to be submitted to industry for comment and ballot.</li> <li>2. The SAR DT has removed references to the Functional Model from the revised SAR.</li> <li>3. The SAR DT has added a list of stakeholder issues for the standard drafting team to address – and updating the FAQ document was added – as an issue for the SDT to address. These additional issues are aggregated into a supplementary SAR that will be posted for industry stakeholder review. The SAR DT modified the SAR to clarify that the interpretation of CIP-006-1 R1.1 shall be addressed.</li> </ol>		
Southwest Power Pool	No	<p>Comments: We generally agree with the scope of the SAR. However, we have the following clarifying questions/comments: The SAR should contain a complete, revised implementation plan for both current and proposed CIP implementation. The SAR indicates that: If additional Functional Model changes are made as a direct result of Order 706 (i.e., Demand Side Aggregator ? see Order 706 paragraph 51), which directly impact</p>

Consideration of Comments on 1st Draft of SAR to Revise Cyber Security Standards — Project 2008-06

Organization	Question 1:	Question 1 Comments:
		<p>the applicable functions, these functional entities will be added to the scope of the cyber security standards resulting from this SAR. Our read of Section 51 shows that FERC has not asked NERC to revise its functional model; it merely directed [?.NERC to register demand side aggregators if the loss of their load shedding capability, for reasons such as a cyber incident, would affect the reliability or operability of the Bulk-Power System.]In our view, registering an organization or group to ensure compliance with reliability standards does not require that organization or group to be defined in the functional model for so long as the functions they register to perform conform with the tasks listed in the model under an appropriate entity. Hence, we do not expect the functional model will be revised to address this directive. As a result, we do not agree that this speculative revision to scope statement should be in the SAR.</p>
<p><b>Response:</b> The STD will develop an implementation plan for the revised standards.</p>		
<p>The SAR DT acknowledges that the LSE is currently identified in the Functional Model as performing load shedding. The SAR DT has removed reference to Functional Model in the revised SAR.</p>		
Ontario IESO	No	<p>1. The SAR is not specific on which CIP standards are "low hanging fruit", which ones contain more contentious issues than the others, and any proposed implementation plan that supports multiple revisions to the standards while some changes are reviewed by industry, balloted, and submitted for approval.</p> <p>2. The SAR indicates that: If additional Functional Model changes are made as a direct result of Order 706 (i.e., Demand Side Aggregator ? see Order 706 paragraph 51), which directly impact the applicable functions, these functional entities will be added to the scope of the cyber security standards resulting from this SAR. Our read of Section 51 shows that FERC has not asked NERC to revise its functional model; it merely dircted [?.NERC to register demand side aggregators if the loss of their load shedding capability, for reasons such as a cyber incident, would affect the reliability or operability of the Bulk-Power System.] In our view, registering an organization or group to ensure compliance with reliability standards does not require that organization or group to be defined in the functional model for so long as the functions they register to perform conform with the tasks listed in the model under an appropriate entity. In this case, we expect the "Demand Side Aggregator", which we believe performs the tasks listed under the LSE in the model, will register as an LSE. Hence, we do not expect the functional model to be revised in order to address this directive. As a result, we do not agree that this speculative revision to the scope statement should be included in the SAR.</p>
<p><b>Response:</b></p> <ol style="list-style-type: none"> <li>The SAR DT agrees that a list of changes to be made to the CIP standards is appropriate for inclusion in the SAR as a scoping reference. It is more appropriate that the SDT determine the timing and grouping of revisions to be submitted to industry for comment and ballot.</li> <li>The SAR DT acknowledges that the LSE is currently identified in the Functional Model as performing load shedding. The SAR DT has</li> </ol>		

Consideration of Comments on 1st Draft of SAR to Revise Cyber Security Standards — Project 2008-06

Organization	Question 1:	Question 1 Comments:
<p><a href="#">removed reference to Functional Model in the revised SAR.</a></p>		
Hydro One Networks Inc.	No	<p>(a) The SAR is not specific on which CIP standards contain more contentious issues than the others, and any proposed implementation plan that supports multiple revisions to the standards while some changes are reviewed by industry, balloted, and submitted for approval.</p> <p>(b) The SAR indicates that: If additional Functional Model changes are made as a direct result of Order 706 (e.g. Demand Side Aggregator ? see Order 706 paragraph 51), which directly impact the applicable functions, these functional entities will be added to the scope of the cyber security standards resulting from this SAR. However, the FERC order has not asked NERC to revise its functional model; it merely directed NERC to register demand side aggregators if the loss of their load shedding capability, for reasons such as a cyber incident, would affect the reliability or operability of the Bulk Power System. In our view, the "Demand Side Agregator" performs tasks that the FM lists under the LSE entity thus it should be registered as such. According to the above, we do not expect the functional model will be revised to address this directive. As a result, we do not agree that this revision to scope statement should be in the SAR.</p>
<p><b>Response:</b></p> <ol style="list-style-type: none"> <li>1. <a href="#">The SAR DT agrees that a list of changes to be made to the CIP standards is appropriate for inclusion in the SAR as a scoping reference. It is more appropriate that the SDT determine the timing and grouping of revisions to be submitted to industry for comment and ballot.</a></li> <li>2. <a href="#">The SAR DT acknowledges that the LSE is currently identified in the Functional Model as performing load shedding. The SAR DT has removed reference to Functional Model in the revised SAR.</a></li> </ol>		
FirstEnergy Corp.	No	<p>See our comments to the rest of the comment form, plus the following:</p> <ol style="list-style-type: none"> <li>1. Although we agree the scope must address the FERC directed changes from Order 706, the SAR must be developed further and lay out a table of all the directives. We look at this first posting of the SAR as just a general starting point for the SAR drafting team who will further develop expectations for the standards drafting team. To aid the SAR drafting team and eventual standards development team, FE has tabulated the FERC directed changes in an Excel spreadsheet that we have submitted separately with these comments to NERC's Barbara Bogenrief. In addition, FE will provide more detailed guidance when the revised SAR is made available for comment.</li> <li>2. It is not clear to FE how the FERC directed changes to the compliance elements such as Violation Factors and Violation Severity Levels will be handled by NERC staff or the eventual CIP standards drafting team. If they are to be addressed by the CIP standards drafting team, then changes to VRFs and VSLs should be included in the SAR scope.</li> </ol>

Consideration of Comments on 1st Draft of SAR to Revise Cyber Security Standards — Project 2008-06

Organization	Question 1:	Question 1 Comments:
<p><b>Response:</b></p> <ol style="list-style-type: none"> <li>The SAR DT thanks the commenter for the summary spreadsheet that accompanied his comments. The SAR DT agrees that a list of changes to be made to the CIP standards is appropriate for inclusion in the SAR as a scoping reference. The drafting team prepared a similar document to the commenter's spreadsheet and it is Attachment #2 of the revised SAR.</li> <li>The Standard Review guide (Attachment #1 of the SAR) that accompanied the posted SAR describes the scope of update work that all standards that come under revision must undergo. Included are the additions or revisions of Violation Risk Factors and Violation Severity Levels.</li> </ol>		
<p>Sempra Energy Trading LLC and Sempra Energy Solutions LLC</p>	<p>No</p>	<p>Sempra Energy Trading LLC and Sempra Energy Solutions LLC disagree with the proposed changes to the applicability section of the Cyber Security Standards (CIP Standards). The expansion of the CIP Standards? applicability to Purchasing-Selling Entities (PSEs) would result in the unnecessary imposition of the CIP Standards on pure power marketers, which are typically registered only as PSEs. The overarching purpose of the CIP Standards is the identification and protection of Critical Cyber Assets, which are those ? Cyber Assets essential to the reliable operation of Critical Assets.? (The Glossary of Terms Used in Reliability Standards, May 2, 2007 at 4 (Glossary) defines Cyber Assets as ?programmable electronic devices and communication networks including hardware, software, and data.?) Entities that do not own or operate any Critical Assets have no Critical Cyber Assets and, therefore, should not be required to comply with the CIP Standards. Pure power marketers engage in power purchase and sale transactions, but do not own or operate any physical electric generation, transmission, or distribution facilities. They also do not own or operate any Critical Assets, which by definition are physical facilities connected to or integrated with the grid. (The Glossary defines Critical Assets as ?facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System.?) As a result, pure power marketers do not own or operate any Critical Cyber Assets and, therefore, should not be required to comply with the CIP Standards. Although power marketers may be users of third-party electronic systems (e.g., OASIS or scheduling systems) that may be considered Critical Cyber Assets, such access is limited to user functions and does not allow in any way marketers (or any other users) to control those Critical Cyber Assets or the underlying physical Critical Assets. Pure power marketers typically qualify and register only as PSEs. The proposed inclusion of PSEs in the applicability section of the CIP Standards would render the CIP Standards applicable to PSEs that are not also owners or operators of physical electric assets, such as power marketers. Such change would impose on such power marketers significant regulatory burdens and costs, without furthering the goals of the CIP Standards. Application of the CIP Standards should be limited to only those functional categories of entities that actually own or control physical electric assets that could be Critical Assets. Such entities are registered with NERC for the proper reliability function that results from the ownership or operation of physical electric assets (including Critical Assets), such as Generator Owner (GO), Generator Operator (GOP), Transmission Owner (TO), or Transmission Operator (TOP). To the extent GOs, GOPs, TOs, and TOPs are included in the applicability section of the CIP Standards, the current exclusion of PSEs from the CIP Standards does not result in any reliability gap, because</p>

Consideration of Comments on 1st Draft of SAR to Revise Cyber Security Standards — Project 2008-06

Organization	Question 1:	Question 1 Comments:
		<p>owners or operators of Critical Cyber Assets are subject to the CIP Standards pursuant to the registration for the functions that relate to their ownership and operation of those physical assets. Indeed, if a power marketer contractually assumes responsibility for the reliability functions associated with the operation of a generator, that marketer will be required to add a GOP registration to its PSE registration. Thus, it appears that the only effect of revising the applicability section of the CIP Standards to include PSEs would be to impose on pure power marketers reliability standards that are not intended to apply to entities that do not own or operate any Critical Assets. The Commission has acknowledged that compliance with the CIP Standards may be difficult and burdensome and has provided for a three year phased implementation. Such burden should not be imposed on entities that do not own or operate Critical Assets and whose compliance with the CIP Standards would not further the reliability of the Bulk Electric System. In the alternative, if NERC revises the applicability section of the CIP Standards to include PSEs, it should qualify the term added in the applicability section to refer only to those PSEs that actually own or control physical electric assets. NERC has previously determined that it is in some cases appropriate to qualify the applicability of a standard to a functional category. For example, reliability standard PRC-016 applies to Transmission Owners, Generator Owners, and Distribution Providers, but its applicability is further limited to include only an entity that owns [a Special Protections System].? As a result, the standard does not apply broadly (and unnecessarily) to every Transmission Owner, Generator Owner, and Distribution Provider. NERC should similarly consider adequate qualifications in the applicability section of the CIP Standards that clearly limit the applicability of the CIP standards to only those PSEs that own or operate physical electric assets.</p>
<p><b>Response:</b> The NERC CIP Cyber Security Standards are applicable to entities that operate or impact the operation of facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System. The SAR DT believes that the PSE serves an economic role, not a reliability role, and that while their systems could be compromised the impact of such compromise would not affect the reliability or operability of the Bulk Electric System due to the other reliability operations controls in place. Therefore the PSE is removed from the SAR as an applicable entity.</p>		
Duke Energy	No	<p>While we agree for the most part with the scope, the Critical Assets are generally Control Centers, Substations, and Critical Generation. What applicability does this standard have for LSE? Is it appropriate that LSE's are included?</p>
<p><b>Response:</b> The SAR DT asserts that LSEs (especially with the capability of shedding load) may have significant effect upon the Bulk Electric System and therefore should be subject to these standards. The CIP-002-1 through CIP-009-1 Standards as currently approved contain requirements that apply to the Load Serving Entity.</p>		
National Institute of Standards and Technology	No	<p>NIST agrees with the proposed changes in FERC Order 706 and proposes several additional items for consideration listed in the comments section of Question 5 of this comment form.</p>

Consideration of Comments on 1st Draft of SAR to Revise Cyber Security Standards — Project 2008-06

Organization	Question 1:	Question 1 Comments:
<b>Response:</b> Thank you for your input. The SAR DT addresses your comments to question #5 below.		
Pacific Gas and Electric Company	No	Please see specific items in questions 2, 4, and 5.
<b>Response:</b> Please see the response to comments on questions 2, 4, and 5.		
Midwest ISO	No	See our answers to the other questions.
<b>Response:</b> Thanks for the input.		
M-S-R Public Power Agency	No	See Question 2 comments.
<b>Response:</b> See our Response to question #2.		
WECC (Steve Rueckert)	No	See specific items in questions 2, 4 & 5
<b>Response:</b> See our Responses to question #2, 4 and 5.		
Ohio Valley Electric Corporation	No	
Oncor Electric Delivery Company LLC	No	
WECC-NERC PMO - PacifiCorp	Yes	Specifically, the scope needs to assure that the NIST standards are considered. Such standards will help organizations overcome confusion where elements of the existing standard is unclear.
<b>Response:</b> The SAR DT agrees. Order 706 directs consideration of NIST standards.		
Ontario Power Generation	Yes	see comments below
<b>Response:</b> The NERC CIP Cyber Security Standards are applicable to entities that operate or impact the operation of facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System. The SAR DT believes that the PSE serves an economic role, not a reliability role, and that while their systems could be compromised the impact of such compromise would not affect the reliability or operability of the Bulk Electric System due to the other reliability operations controls in place. Therefore the PSE is removed from the SAR as an applicable entity.		
Coral Power,	Yes	Assuming the question should read: "Do you agree with the scope of the proposed standards action ?" The

## Consideration of Comments on 1st Draft of SAR to Revise Cyber Security Standards — Project 2008-06

Organization	Question 1:	Question 1 Comments:
L.L.C.		scope of the SAR is reasonable, since it is to address the directives of Order 706. Yet, this needs to be differentiated from the proposal in the SAR to expand the scope of applicable entities to include the Regional Entity and Purchasing-selling Entity. Inclusion of PSEs was not directed in the Order, or even considered as part of the NOPR, and should be removed from the SAR.
<p><b>Response:</b> The NERC CIP Cyber Security Standards are applicable to entities that operate or impact the operation of facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System. The SAR DT believes that the PSE serves an economic role, not a reliability role, and that while their systems could be compromised the impact of such compromise would not affect the reliability or operability of the Bulk Electric System due to the other reliability operations controls in place. Therefore the PSE is removed from the SAR as an applicable entity.</p>		
We Energies	Yes	We Energies feels that incorporating the FERC 706 directives will provide additional clarity around implementation requirements and compliance measures to the existing CIP 002-009 standards.
<p><b>Response:</b> Thank you for your input.</p>		
Electric Power Supply Association	Yes	Yes. To the extent that the proposed SAR incorporates actions identified in FERC Order 706, the scope is appropriate. Given the recent, very thorough vetting of this issue through the FERC NOPR and Order process, the Standards Drafting Team should be very cautious about any extensions to that scope.
<p><b>Response:</b> The SAR DT thanks the commenter for its input. Extensions to the scope will be determined by industry input as submitted to question #5 and #6.</p>		
ElectriCities of North Carolina, Inc.	Yes	However, do not agree with expanding the scope of applicability as stated (see <b>Response</b> to Q2).
<p><b>Response:</b> The NERC CIP Cyber Security Standards are applicable to entities that operate or impact the operation of facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System. The SAR DT believes that the PSE serves an economic role, not a reliability role, and that while their systems could be compromised the impact of such compromise would not affect the reliability or operability of the Bulk Electric System due to the other reliability operations controls in place. Therefore the PSE is removed from the SAR as an applicable entity.</p>		
Southern Company Services, Inc.	Yes	Please see our comment to Question #2.
<p><b>Response:</b> Please refer to our <a href="#">Response to Question #2</a></p>		
LK4 Technology Corporation	Yes	The industry needs to adopt a common risk assessment methodology. As a veteran compliance auditor for FFIEC, GLBA and SarBox, I have seen entire compliance programs disallowed because they did not start with

Consideration of Comments on 1st Draft of SAR to Revise Cyber Security Standards — Project 2008-06

Organization	Question 1:	Question 1 Comments:
		the risk assessment. The NRC recently commissioned a cybersecurity risk assessment program and is in the process of commissioning a physical risk assessment. These risk assessments can be personalized for each individual complying entity, but a core criteria must be met by all.
<p><b>Response:</b> Thank you for your input. The standard drafting team is tasked with improving the clarity in the standards as part of the revision work scope. As a supplement to aid in understanding the current CIP standards, the CIPC Risk Assessment Working Group is drafting guidance for use by the industry. This guidance will be posted for public comment and the SAR DT respectfully invites the commenter to review the guideline as it becomes available.</p>		
PJM Interconnection	Yes	
Detroit Edison	Yes	
PPL Generation, LLC	Yes	
American Electric Power	Yes	
United Illuminating	Yes	
AEP	Yes	
Western Electricity Coordinating Council	Yes	
Dominion Resources Services, Inc.	Yes	
Public Service Commission of South Carolina	Yes	

## Consideration of Comments on 1st Draft of SAR to Revise Cyber Security Standards — Project 2008-06

2. This SAR proposes to add the Regional Entities and Purchasing-Selling Entity functions to the applicability section of the revised standards. If additional Functional Model changes are made (or if changes are made to the Compliance Registration Criteria) as a direct result of Order 706 (i.e., Demand Side Aggregator — see Order 706 paragraph 51), which directly impact the applicable functions, conforming modifications will be made to the cyber security standards. Do you agree with these proposed changes to the applicability sections of these standards?

Summary Consideration: Nearly all the respondents believed that Purchasing Selling Entities should not be subject to the Cyber Security standards. The SAR DT agrees and has removed PSEs from the applicability section of the revised SAR. Several commenters indicated that the reference to the Functional Model should be removed because the FERC Order did not reference the Functional Model and because the tasks assigned to the Demand Side Aggregator are performed by the Load-serving Entity. The drafting team agrees that the tasks assigned to the Demand Side Aggregator are performed by the Load-serving Entity, and the reference in the SAR to the Functional Model modifications has been removed. The SAR already identifies the Load-serving Entity as having responsibilities for some requirements in CIP-002-1 through CIP-009-1.

Organization	Question 2:	Question 2 Comments:
Xcel Energy	No	As noted above, we do not believe that any justification has been provided for extending the reach of the CIP standards to PSEs.
<p><b>Response:</b> The NERC CIP Cyber Security Standards are applicable to entities that operate or impact the operation of facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System. The SAR DT believes that the PSE serves an economic role, not a reliability role, and that while their systems could be compromised the impact of such compromise would not affect the reliability or operability of the Bulk Electric System due to the other reliability operations controls in place. Therefore the PSE is removed from the SAR as an applicable entity.</p>		
Ontario Power Generation	No	I see no need to expand the applicability of the CIP Standards to PSEs. This appears to be an indirect method of including market data - a subject that was contemplated within FERC's NOPR and widely opposed.
<p><b>Response:</b> The NERC CIP Cyber Security Standards are applicable to entities that operate or impact the operation of facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System. The SAR DT believes that the PSE serves an economic role, not a reliability role, and that while their systems could be compromised the impact of such compromise would not affect the reliability or operability of the Bulk Electric System due to the other reliability operations controls in place. Therefore the PSE is removed from the SAR as an applicable entity.</p>		
PPL Generation, LLC	No	PPL Supply disagrees with the intent to add the PSE function to the CIP applicability. It is not clear to PPL how the transactions by a PSE would involve critical cyber assets essential to the reliable operations of the BPS.
<p><b>Response:</b> The NERC CIP Cyber Security Standards are applicable to entities that operate or impact the operation of facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System. The SAR DT believes that the PSE serves an economic role, not a reliability role, and that while their systems could be compromised the impact of such compromise would not affect the reliability or operability of the Bulk Electric System due to the other reliability operations controls in place.</p>		

Consideration of Comments on 1st Draft of SAR to Revise Cyber Security Standards — Project 2008-06

Organization	Question 2:	Question 2 Comments:
<p>Therefore the PSE is removed form the SAR as an applicable entity.</p>		
<p>Pacific Gas and Electric Company</p>	<p>No</p>	<p>Paragraph 4 of the SAR isn't clear. Assuming that the proposal of this paragraph, and it's bullets, is directly related to FERC Order 706 Paragraph 272, we would recommend rewording to:"This SAR will provide clairty in identifying various types of assets that feed information to critical assets used to support the reliability and operability of the Bulk-Power System as directed in FERC Order 706 Paragraph 272. This includes how to address: - Regional Entities and Purchasing-Selling Entity functions as they relate to the reliability and operability of the Bulk-Power System. - Reliability and Market Interface Principle 4 (plans for emergency operations and system restoration).</p>
<p><b>Response:</b> The NERC CIP Cyber Security Standards are applicable to entities that operate or impact the operation of facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System. The SAR DT believes that the PSE serves an economic role, not a reliability role, and that while their systems could be compromised the impact of such compromise would not affect the reliability or operability of the Bulk Electric System due to the other reliability operations controls in place. Therefore the PSE is removed form the SAR as an applicable entity.                      The Regional Entities are subject to standards through the Delegation Agreements with NERC.</p>		
<p>Coral Power, L.L.C.</p>	<p>No</p>	<p>Making the standards applicable to the Regional Entity function was in the NOPR, commented on by stakeholders, considered by FERC and determined to be appropriate (paragraph 47). A great deal of discussion and consideration went to addressing comments and concerns regarding demand side aggregators, concluding with the direction that NERC should consider whether there is a need to register such entities and, if so, to address related issues and develop criteria for their registration (paragraph 51). As such, it is easy to agree that the applicability sections of the standards should be changed in line with the Order. However, nowhere, in this Order or in the NOPR, did FERC propose or contemplate or even discuss the inclusion of PSEs as responsible entities for the CIP standards. If there were any concerns related to PSEs they would have been raised by FERC and/or pursued by stakeholders, similar to those regarding small entities. FERC considered this, and determined that it would be "overly-expansive" to require every entity connected to the Bulk-Power System, to comply with the CIP standards, regardless of size (paragraph 49). PSEs, of course, are not even connected to the BPS. In reaffirming its reliance on the NERC registration process to identify entities that should comply with the CIP standards, FERC was not directing NERC to go back and make them apply to more entities, like PSEs. On the contrary, in listing all of the responsible entities that must comply with the CIP standards in paragraph 31, it is clear that FERC knew exactly which entities the standards do not - and should not - apply to. There is no explanation or support within the SAR describing the logic or reliability reasons for making PSEs responsible entities under the CIP standards. The only justification appears to be the desire to address the directives of FERC in Order 706, but there is no such directive to include PSEs. The SAR should be amended to eliminate the expansion of the applicability to PSEs.</p>
<p><b>Response:</b> The NERC CIP Cyber Security Standards are applicable to entities that operate or impact the operation of facilities, systems, and</p>		

**Consideration of Comments on 1st Draft of SAR to Revise Cyber Security Standards — Project 2008-06**

Organization	Question 2:	Question 2 Comments:
		<p>equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System. The SAR DT believes that the PSE serves an economic role, not a reliability role, and that while their systems could be compromised the impact of such compromise would not affect the reliability or operability of the Bulk Electric System due to the other reliability operations controls in place. Therefore the PSE is removed form the SAR as an applicable entity.</p>
AEP	No	<p>In general a PSE has no direct control on system (e.g. OASIS, organized Market Applications) and/or the grid, and relevant transactions are ultimately approved or denied by a current reliability function such as the Interchange Authority, Balancing Authority and Reliability Coordinator. The PSE function was originally (and still is) designed in the context of the physical scheduling process to assign financial responsibility in the related contract path represented on an eTAG. A PSE neither creates load or generation, and at all times only serves as an intermediary, in a bilateral transaction, to schedule generation to load. There is already enormous confusion as to what an LSE does (Market based functions vs. Reliability based functions), and in reality, what FERC references in Order 706 best aligns with the LSE function, definitely not a PSE function, so lets not further confuse the issue by wrongly including the PSE function in this debate.</p>
		<p><b>Response:</b> The NERC CIP Cyber Security Standards are applicable to entities that operate or impact the operation of facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System. The SAR DT believes that the PSE serves an economic role, not a reliability role, and that while their systems could be compromised the impact of such compromise would not affect the reliability or operability of the Bulk Electric System due to the other reliability operations controls in place. Therefore the PSE is removed form the SAR as an applicable entity.</p>
ElectriCities of North Carolina, Inc.	No	<p>By definition, the PSE purchases or sells, and takes title to, energy, capacity, and Interconnected Operations Services. To accomplish that, it would have to work through other entities (TSPs, BAs, TOPs, GOPs, etc.) that are already required to meet the cyber security standards and that DO have responsibilities for managing and operating the facilities and processes that actually impact the reliability of the BES. If the PSE happens to be an affiliated merchant or a generator owner itself, then in addition to being registered as a PSE, that entity should also be registered according to the other functions it performs and would have to comply with the cyber security standards on those registration bases. It does not make sense to extend registration to PSEs, or any other functional entity, whose function itself does not physically impact the reliability of the BES.</p>
		<p><b>Response:</b> The NERC CIP Cyber Security Standards are applicable to entities that operate or impact the operation of facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System. The SAR DT believes that the PSE serves an economic role, not a reliability role, and that while their systems could be compromised the impact of such compromise would not affect the reliability or operability of the Bulk Electric System due to the other reliability operations controls in place. Therefore the PSE is removed form the SAR as an applicable entity.</p>
Ontario IESO	No	<p>We concur that the Regional Entities should be added to the applicability section, but not the Purchasing-Selling</p>

Consideration of Comments on 1st Draft of SAR to Revise Cyber Security Standards — Project 2008-06

Organization	Question 2:	Question 2 Comments:
		<p>Entities. Regional Reliability Organizations were included as applicable entities in the previously submitted CIP standards; the proposal to include the RE is a only matter of name change with respect to the revised Functional Model. However, we do not agree with adding PSE to the applicability section. The PSEs are basically commercial entities; we are unable to identify which tasks they perform that would have an impact on critical infrastructure protection, nor can we find its inclusion stipulated in the FERC Order.</p> <p>With respect to the proposal to make conforming changes to the cyber security standards if additional Functional Model changes are made (or if changes are made to the Compliance Registration Criteria), please see our comments on Q1. Furthermore, we have difficulty understanding the need to change reliability standards if the Compliance Registration Criteria are changed. We would assume that the reliability standards stipulate the requirements, and assign them to the applicable entities. The Compliance Registration Criteria would provide the conditions for those organizations/persons/entities who perform the tasks listed under the functional entities in the Functional Model to register as such (Functional Entity). We are unable to see how the Compliance Registration Criteria would precipitate a need to change the standards, which to us is a reverse process.</p>
<p><b>Response:</b> The NERC CIP Cyber Security Standards are applicable to entities that operate or impact the operation of facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System. The SAR DT believes that the PSE serves an economic role, not a reliability role, and that while their systems could be compromised the impact of such compromise would not affect the reliability or operability of the Bulk Electric System due to the other reliability operations controls in place. Therefore the PSE is removed form the SAR as an applicable entity.</p>		
<p>Regarding Compliance Registry Criteria, the drafting team agrees it should not precipitate a change to the standards and has removed reference to the Functional Model from the SAR.</p>		
Hydro One Networks Inc.	No	<p>(a) We concur that the Regional Entities should be added to the applicability section, but not the Purchasing-Selling Entities. However, clarification must be sought from FERC because Regional Entities are not Owners, Users or Operators of the BPS, thus not legally subject to reliability standards</p> <p>(b) We do not agree with adding PSE to the applicability section. The PSEs are basically commercial entities and we are unable to identify which tasks they perform that would have an impact on critical infrastructure protection, nor can we find its inclusion stipulated in the FERC Order.</p> <p>(c) With respect to the proposal to make conforming changes to the CIP standards if additional Functional Model changes are made (or if changes are made to the Compliance Registration Criteria), please see our comments in Question 1. Furthermore, we do not agree with the need to change reliability standards if the Compliance</p>

Consideration of Comments on 1st Draft of SAR to Revise Cyber Security Standards — Project 2008-06

Organization	Question 2:	Question 2 Comments:
		<p>Registration Criteria are changed. We would assume that the reliability standards stipulate the requirements, and assign them to the applicable entities. The Compliance Registration Criteria would provide the conditions for those organizations/persons/entities who perform the tasks listed under the functional entities in the Functional Model to register as such (Functional Entity). We do not believe that changes the Compliance Registration Criteria would trigger a need to change the standards.</p>
<p><b>Response:</b></p> <ul style="list-style-type: none"> <li>a. The Regional Entities are subject to standards through the Delegation Agreements with NERC.</li> <li>b. The NERC CIP Cyber Security Standards are applicable to entities that operate or impact the operation of facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System. The SAR DT believes that the PSE serves an economic role, not a reliability role, and that while their systems could be compromised the impact of such compromise would not affect the reliability or operability of the Bulk Electric System due to the other reliability operations controls in place. Therefore the PSE is removed from the SAR as an applicable entity.</li> <li>c. Regarding Compliance Registry Criteria, the drafting team agrees it should not precipitate a change to the standards and has removed reference to the Functional Model from the SAR.</li> </ul>		
NPCC	No	<p>The SAR should remove the applicability to the RE. The RE is not a user owner or operator and does not have Critical Cyber Assets that control the BPS.</p> <p>We do not agree with adding PSE to the applicability section. The PSEs are basically commercial entities; we are unable to identify which tasks they perform that would have an impact on critical infrastructure protection, nor can we find its inclusion stipulated in the FERC Order.</p> <p>With respect to the proposed to make conforming changes to the cyber security standards if additional Functional Model changes are made (or if changes are made to the Compliance Registration Criteria), please refer to the comments above in Question 1. Furthermore, we have difficulty understanding the need to change reliability standards if the Compliance Registration Criteria are changed. We would assume that the reliability standards stipulate the requirements, and assign them to the applicable entities. The Compliance Registration Criteria would provide the conditions for those organizations/persons/entities who perform the tasks listed under the functional entities in the Functional Model to register as such (Functional Entity). We are unable to see how the Compliance Registration Criteria would precipitate a need to change the standards, which to us is a reverse process.</p>
<p><b>Response:</b> The NERC CIP Cyber Security Standards are applicable to entities that operate or impact the operation of facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System.</p> <p>The Regional Entities do have an “impact on the operation of facilities, systems and equipment. . .” and are subject to standards through the</p>		

**Consideration of Comments on 1st Draft of SAR to Revise Cyber Security Standards — Project 2008-06**

Organization	Question 2:	Question 2 Comments:
<p>Delegation Agreements with NERC.</p> <p>The SAR DT believes that the PSE serves an economic role, not a reliability role, and that while their systems could be compromised the impact of such compromise would not affect the reliability or operability of the Bulk Electric System due to the other reliability operations controls in place. Therefore the PSE is removed form the SAR as an applicable entity.</p> <p>Regarding Compliance Registry Criteria, the drafting team agrees it should not precipitate a change to the standards and has removed reference to the Functional Model from the SAR.</p>		
Ohio Valley Electric Corporation	No	Regional Entities are not users, owners or operators of the Bulk Electric System and thus the reliability standards do not apply to them by definition. It is not clear why the LSE and PSE are to be included. LSEs and PSEs do not own any Critical Assesets that directly affect the bulk electric system. Subsequently, these entities could not have any Critical Cyber Assets.
<p><b>Response:</b> The NERC CIP Cyber Security Standards are applicable to entities that operate or impact the operation of facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System. The Regional Entities do have an “impact on the operation of facilities, systems and equipment. . .” and are subject to standards through the Delegation Agreements with NERC.</p> <p>The SAR DT believes that the PSE serves an economic role, not a reliability role, and that while their systems could be compromised the impact of such compromise would not affect the reliability or operability of the Bulk Electric System due to the other reliability operations controls in place. Therefore the PSE is removed form the SAR as an applicable entity.</p> <p>Load-serving Entities are already identified as a responsible entity for requirements in CIP-002-1 through CIP-009-1.</p>		
Midwest ISO	No	Regional Entities are not users, owners or operators of the Bulk Electric System. Thus, reliability standards can't apply to them by statute. It is not clear why the LSE and PSE are included. The LSE and PSE will not own any Cyber Assets that directly affect Critical Assets. Thus, it is not possible for them to have Critical Cyber Assets.
<p><b>Response:</b> The NERC CIP Cyber Security Standards are applicable to entities that operate or impact the operation of facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System.</p> <p>The Regional Entities do have an “impact on the operation of facilities, systems and equipment. . .” and are subject to standards through the Delegation Agreements with NERC.</p> <p>The SAR DT believes that the PSE serves an economic role, not a reliability role, and that while their systems could be compromised the impact of such compromise would not affect the reliability or operability of the Bulk Electric System due to the other reliability operations controls in place. Therefore the PSE is removed form the SAR as an applicable entity.</p>		

Consideration of Comments on 1st Draft of SAR to Revise Cyber Security Standards — Project 2008-06

Organization	Question 2:	Question 2 Comments:
<p>Load-serving Entities are already identified as a responsible entity for requirements in CIP-002-1 through CIP-009-1.</p>		
Dominion Resources Services, Inc.	No	The FERC order stated "that demand side aggregators might also need to be included in the NERC registration process if their load shedding capacity would affect the reliability or operability of the Bulk-Power System. The current version of NERC functional model definition of PSE does not contain any reference to load shed capability, which is the focus of FERC's comment. As we've stated in comments to other standards, the ability to shed load lies with the asset owner of the physical infrastructure.
<p><b>Response:</b> The NERC CIP Cyber Security Standards are applicable to entities that operate or impact the operation of facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System. The SAR DT believes that the PSE serves an economic role, not a reliability role, and that while their systems could be compromised the impact of such compromise would not affect the reliability or operability of the Bulk Electric System due to the other reliability operations controls in place. Therefore the PSE is removed from the SAR as an applicable entity.</p>		
Oncor Electric Delivery Company LLC	No	Oncor Electric Delivery does not agree that the Demand Side Aggregator should be a registered Entity subject to the NERC CIP standard. For purposes of Load Shedding within ERCOT, Oncor Electric Delivery performs this function as directed in ERCOT's Guides and Protocols.
<p><b>Response:</b> The SAR DT acknowledges that the LSEs are currently identified in the Functional Model as performing load shedding. The SAR DT has removed reference to Functional Model in the revised SAR.</p>		
Electric Power Supply Association	No	No. The SAR notes that based on a previous SAR, finalized on March 8, 2004, they intend to expand the applicability to include PSEs. EPSA does not agree with this addition. FERC Order 706 makes no suggestion that such an expansion of the applicability is appropriate. Indeed in Paragraph 31 of the Order, they note the 11 Functional Model entities that they believe are covered by the Order and PSEs are not included. If there was an intent to expand the applicability of the Standards, based on a 2004 SAR, it would have been appropriate to raise that issue during the FERC procedure.
<p><b>Response:</b> The NERC CIP Cyber Security Standards are applicable to entities that operate or impact the operation of facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System. The SAR DT believes that the PSE serves an economic role, not a reliability role, and that while their systems could be compromised the impact of such compromise would not affect the reliability or operability of the Bulk Electric System due to the other reliability operations controls in place. Therefore the PSE is removed from the SAR as an applicable entity.</p>		
M-S-R Public Power Agency	No	M-S-R Public Power Agency ("M-S-R") has determined that the SAR's proposal to add Purchasing-Selling Entities ("PSE") to the applicability section of the revised standards is out of scope and inappropriate. NERC's announcement for this comment period states that "The SAR proposes to bring the following standards (i.e. CIP-

Consideration of Comments on 1st Draft of SAR to Revise Cyber Security Standards — Project 2008-06

Organization	Question 2:	Question 2 Comments:
		<p>002-1 through CIP-009-1) into conformance with the ERO Rules of Procedure and to address the directives from FERC Order 706," but our review of these documents finds no suggestions, let alone directives, indicating that these standards should become applicable to PSE. In Order 706 at Paragraph 49, FERC cautions against an "overly-expansive" approach "requiring that any entity connected to the Bulk-Power System, regardless of size, must comply with the CIP Reliability Standards irrespective of the NERC registry." M-S-R contends that the PSE function in and of itself does not involve any Critical Assets, let alone Critical Cyber Assets and therefore concludes that the proposed PSE applicability of the revised standards is inappropriate. In its "Glossary of Terms Used in Reliability Standards" as adopted by the NERC Board of Trustees on February 12, 2008, NERC provides the following definitions of terms essential to the applicability of the CIP standards: Critical Assets: Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System. Cyber Assets: Programmable electronic devices and communication networks including hardware, software, and data. Critical Cyber Assets: Cyber Assets essential to the reliable operation of Critical Assets. While an entity's business practices related to the PSE function may involve confidential information related to power contracts and prices and this information may be resident on Cyber Assets, there is no manner in which these assets could affect the reliability or operability of the Bulk Electric System if destroyed, degraded, or otherwise rendered unavailable. Adding PSE to the applicability section of the revised standards would cause every entity registered as a PSE to comply with the requirements of CIP-002 only to annually confirm that it has no Critical Cyber Assets. Such an exercise would be unnecessarily burdensome to entities that are already incurring high costs to comply with the appropriately applicable standards.</p>
<p><b>Response:</b> The NERC CIP Cyber Security Standards are applicable to entities that operate or impact the operation of facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System. The SAR DT believes that the PSE serves an economic role, not a reliability role, and that while their systems could be compromised the impact of such compromise would not affect the reliability or operability of the Bulk Electric System due to the other reliability operations controls in place. Therefore the PSE is removed from the SAR as an applicable entity.</p>		
WECC (Steve Rueckert)	No	<p>Paragraph 4 of the Detailed Description section in the SAR isn't clear. Assuming that the intent of this paragraph is directly related to FERC Order 706 Paragraph 272, recommend revising the section to reflect that the scope of the drafting effort: Provide clarity in identifying various types of assets that feed information to critical assets used to support the reliability and operability of the Bulk-Power System as directed in FERC Order 706 Paragraph 272. This includes how to address: - Regional Entities and Purchasing-Selling Entity functions as they relate to the reliability and operability of the Bulk-Power System. - Reliability and Market Interface Principle 4 (plans for emergency operations and system restoration).?</p>
<p><b>Response:</b> The NERC CIP Cyber Security Standards are applicable to entities that operate or impact the operation of facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System. The SAR DT believes that the PSE serves an economic role, not a reliability role, and that while their systems could be compromised the impact of</p>		

**Consideration of Comments on 1st Draft of SAR to Revise Cyber Security Standards — Project 2008-06**

Organization	Question 2:	Question 2 Comments:
<p>such compromise would not affect the reliability or operability of the Bulk Electric System due to the other reliability operations controls in place. Therefore the PSE is removed from the SAR as an applicable entity.</p> <p>The Regional Entities are subject to standards through the Delegation Agreements with NERC.</p>		
Southwest Power Pool	No	<p>Comments: We concur that the Regional Entities should be added to the applicability section, but not the Purchasing-Selling Entities. Regional Reliability Organizations were included as applicable entities in previously submitted CIP standards; the proposal to include the RE is a matter of name change. However, we do not agree with adding PSE to the applicability section. The PSEs are basically commercial entities; we are unable to identify which tasks they perform that would have an impact on Critical Assets, nor can we find its inclusion stipulated in the FERC Order. Wrt the proposed to make conforming changes to the cyber security standards if additional e our comments on Q1.</p> <p>Furthermore, we have difficulty understanding the need to change reliability standards if the Compliance Registration Criteria are changed. We would assume that the reliability standards stipulate the requirements, and assign them to the applicable entities. The Compliance Registration Criteria would provide the conditions for those organizations/persons/entities who perform the tasks listed under the functional entities in the Functional Model to register as such (Functional Entity). We are unable to see how the Compliance Registration Criteria would precipitate a need to change the standards, which to us is a reverse process.</p>
<p><b>Response:</b> The NERC CIP Cyber Security Standards are applicable to entities that operate or impact the operation of facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System. The SAR DT believes that the PSE serves an economic role, not a reliability role, and that while their systems could be compromised the impact of such compromise would not affect the reliability or operability of the Bulk Electric System due to the other reliability operations controls in place. Therefore the PSE is removed from the SAR as an applicable entity.</p> <p>Regarding Compliance Registry Criteria, the drafting team agrees it should not precipitate a change to the standards and has removed reference to the Functional Model from the SAR.</p>		
Sempra Energy Trading LLC and Sempra Energy Solutions LLC	No	See answer to Question 1
<p><b>Response:</b> The NERC CIP Cyber Security Standards are applicable to entities that operate or impact the operation of facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System. The SAR DT believes that the PSE serves an economic role, not a reliability role, and that while their systems could be compromised the impact of</p>		

**Consideration of Comments on 1st Draft of SAR to Revise Cyber Security Standards — Project 2008-06**

Organization	Question 2:	Question 2 Comments:
		such compromise would not affect the reliability or operability of the Bulk Electric System due to the other reliability operations controls in place. Therefore the PSE is removed form the SAR as an applicable entity.
Southern Company Services, Inc.	Yes	We agree with the RE and PSE additions if it makes sense. However, if the drafting team feels that this is not appropriate remove it As to the DSM function, it appears that this is just a subset of the LSE function and this is just a market function. The drafting team should consider if this is a duplicative function of the LSE.
		<p><b>Response:</b> The NERC CIP Cyber Security Standards are applicable to entities that operate or impact the operation of facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System. The SAR DT believes that the PSE serves an economic role, not a reliability role, and that while their systems could be compromised the impact of such compromise would not affect the reliability or operability of the Bulk Electric System due to the other reliability operations controls in place. Therefore the PSE is removed form the SAR as an applicable entity.</p> <p>The Regional Entities are subject to standards through the Delegation Agreements with NERC.</p> <p>The SAR DT acknowledges that the LSEs are currently identified in the Functional Model as performing load shedding. The SAR DT has removed reference to Functional Model in the revised SAR.</p>
LK4 Technology Corporation	Yes	A cyber security system is only as strong as its weakest link. Having unaudited systems interfacing with complying systems represents a large identifiable risk.
		<p><b>Response:</b> The SAR DT thanks you for your comment. The standards CIP-005 and CIP -007 address the types of issues you refer to in your comment. Use of an electronic security perimeter (ESP) implies a mutual distrust posture that requires each responsible entity that has identified critical cyber assets to protect itself and not trust any communication crossing an ESP regardless of where that communication originates.</p>
FirstEnergy Corp.	Yes	The CIP standards should be adjusted to cover any and all functional entities that can impact the reliable operations of the BES. The CIP standards should be adjusted to focus on entities who own cyber entry points that can lead to a compromised BES. Presently the CIP-002 standard is focused on identification of critical BES assets (transmission/generation) and then reviewing those assets for critical cyber assets. This approach could exclude functional entities that do not own BES assets but have an impact on the reliable operation of BES assets.
		<p><b>Response:</b> The SAR DT thanks you for your input. The standard drafting team is tasked with improving the clarity in the standards as part of the revision work scope. As a supplement to aid in understanding the current CIP standards, the CIPC Risk Assessment Working Group is drafting guidance for use by the industry. This guidance will be posted for public comment and the SAR DT respectfully invites the commenter to review the guideline as it becomes available. Applicability of the CIP Standards to any entity with cyber entry points as a criterion for who should be subject to these requirements has merit. Attachment #1 of the SAR allows for review of the Applicability section of these standards to ensure there are no overlaps or gaps.</p>
PJM Interconnection	Yes	

Consideration of Comments on 1st Draft of SAR to Revise Cyber Security Standards — Project 2008-06

Organization	Question 2:	Question 2 Comments:
Detroit Edison	Yes	
American Transmission Company	Yes	
American Electric Power	Yes	
United Illuminating	Yes	
National Institute of Standards and Technology	Yes	
We Energies	Yes	
Western Electricity Coordinating Council	Yes	
Duke Energy	Yes	
Public Service Commission of South Carolina	Yes	

## Consideration of Comments on 1st Draft of SAR to Revise Cyber Security Standards — Project 2008-06

3. If you are aware of any regional variances or associated business practices that we should consider with this SAR please identify them here.

Summary Consideration: None of the commenters are aware of any regional variances or associated business practices as they pertain to Cyber Security. The SAR DT agrees that there should be uniform technical requirements and consistent auditing of these requirements across regions.

Organization	Regional Variance	Business Practice:
Xcel Energy	As noted above, the rationale for applying the CIP standards to PSEs has not been provided. Absent an understanding of the reasons for pulling PSEs within the ambit of the CIP standards, we are unable to comment on the need for any regional or business practice variance.	
<p><b>Response:</b> The NERC CIP Cyber Security Standards are applicable to entities that operate or impact the operation of facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System. The SAR DT believes that the PSE serves an economic role, not a reliability role, and that while their systems could be compromised the impact of such compromise would not affect the reliability or operability of the Bulk Electric System due to the other reliability operations controls in place. Therefore the PSE is removed from the SAR as an applicable entity.</p>		
PJM Interconnection	Regional variances should be few if any. The Regional Entities will need to apply compliance guidelines consistently across the U.S. in order to circumvent issues with inconsistency.	
<p><b>Response:</b> The SAR DT thanks you for your input with respect to regional variances. The team asserts that there should be uniform technical requirements and consistent auditing of these requirements across regions.</p>		
American Transmission Company	ATC is not aware of any regional or business variance that the SDT should consider.	
We Energies	We Energies is not aware of any regional or business variance that the standards team should consider.	
Southern Company Services, Inc.	We know of no regional variances to identify at this point. However, if at some point in time the drafting team feels one is necessary they should consider adding it.	
Pacific Gas and Electric Company	None	
M-S-R Public Power Agency	None.	
WECC (Steve Rueckert)	none	

Consideration of Comments on 1st Draft of SAR to Revise Cyber Security Standards — Project 2008-06

4. Do you agree with the “multi-phase” approach identified in the SAR? (The SAR’s proposal is to take the easiest modifications through the posting and balloting cycles first, followed by one or more sets of modifications to address those directives that will take more time.)

Summary Consideration: The comments ranged from agreement with to cautious opposition to a “multi-phase” approach to this project. The SAR DT believes that the SDT ought to adopt the optimal approach on their own accord as they will be in the best position to determine work approach. Therefore the SAR will not constrain the SDT to adopting a multi-phase approach but instead provide the SDT the latitude to choose one in order to accomplish the objectives set forth in the SAR.

Organization	Question 4:	Question 4 Comments:
Xcel Energy	No	Any further changes to the CIP standards should be proposed and adopted on a comprehensive basis. The piecemeal approach contemplated in this question creates a significant risk that changes adopted in one cycle could be altered or overridden by changes approved in a subsequent cycle, undermining the ability of stakeholders to efficiently and effectively manage costs of implementing the CIP standards. The industry is engaged in a very substantial effort to ramp up to comply with the existing standards. This effort will result in substantial additional costs to companies and consumers. While this effort is ongoing, the CIP landscape is continuing to change, creating the very real possibility that work that is currently ongoing will become obsolete with the next round of CIP standards. The current situation will only be exacerbated if the next phase of the CIP standards are adopted on a piecemeal basis.
<p><b>Response:</b> The SDT is best positioned to determine if a multi-phased approach is appropriate and if yes the timing and grouping of revisions to be submitted to the industry for comment and ballot. The multi-phased approach is an option (not a requirement). Should the SDT deem another approach to be superior it has the latitude to proceed as such.</p>		
Detroit Edison	No	A "multi-phase" approach is a sound idea for a task of this magnitude however, the order of modifications should be based on priority rather than ease of implementation. FERC Order 706 clearly stated that "Reasonable Business Judgment" (P138) and "Acceptance of Risk" (P150) need to be removed and "Technical Feasibility" exceptions need to have criteria developed to ensure accountability (P222). The first two would most likely fall into the easy category and the third might not. The "Technical Feasibility" language used by FERC indicates that it should be high on the priority list and should not be delayed because it may be difficult to address. Other high priority issues should include Periodic Self Certifications (P96). The drafting team should consider all of FERC's comments, determine priorities, and plan a revision schedule based on those priorities
<p><b>Response:</b> The SDT is best positioned to determine if a multi-phased approach is appropriate and if yes the timing and grouping of revisions to be submitted to the industry for comment and ballot. The multi-phased approach is an option (not a requirement). Should the SDT deem another approach to be superior it has the latitude to proceed as such.</p>		

## Consideration of Comments on 1st Draft of SAR to Revise Cyber Security Standards — Project 2008-06

Organization	Question 4:	Question 4 Comments:
Ontario Power Generation	No	The multi-phase approach appears cumbersome and confusing. The standards will be in a perpetual state of flux and members will have a more difficult time implementing programs to ensure compliance against a moving target. Modifications should be done in a comprehensive fashion.
<p><b>Response:</b> The SDT is best positioned to determine if a multi-phased approach is appropriate and if yes the timing and grouping of revisions to be submitted to the industry for comment and ballot. The multi-phased approach is an option (not a requirement). Should the SDT deem another approach to be superior it has the latitude to proceed as such.</p>		
Ohio Valley Electric Corporation	No	Registered entities have already been working towards compliance with the CIP standards per the existing implementation plan. The drafting team is now proposing to make changes before the existing implementation plan is complete. Registered entities need to be allowed to become compliant with the existing standards before additional changes are made to the CIP standards. Otherwise, the drafting team is creating a moving target that provides an incentive to delay implementation right up until an entity is required to be auditably compliant. By delaying their implementation, registered entities could save costs from having to make multiple changes to meet changing CIP requirements without incurring penalties. FERC confirmed in Order 706 that no penalties could be applied until the auditably compliant phase. The drafting team should list the required changes from FERC Order 706 directly in the SAR and what class they consider the change to be in. Also, if additional and acceptable changes are requested from the commentors, these changes should be listed in the SAR and clearly marked as coming from industry.
<p><b>Response:</b> The SDT is best positioned to determine if a multi-phased approach is appropriate and if yes the timing and grouping of revisions to be submitted to the industry for comment and ballot. The multi-phased approach is an option (not a requirement). Should the SDT deem another approach to be superior it has the latitude to proceed as such.</p>		
PPL Generation, LLC	No	PPL Supply disagrees with the SDT's approach to addressing issues through multiple revisions. This approach will add complexity and rapid changes to the standards making it difficult for entities dealing with implementing plans, some with long lead-times, to be compliant with the changing requirements.
<p><b>Response:</b> The SDT is best positioned to determine if a multi-phased approach is appropriate and if yes the timing and grouping of revisions to be submitted to the industry for comment and ballot. The multi-phased approach is an option (not a requirement). Should the SDT deem another approach to be superior it has the latitude to proceed as such.</p>		
Pacific Gas and Electric Company	No	In theory it is a reasonable approach if the first phase only consist of simple changes to reporting timeframes, etc. that don't have any interrelation or complexity to controversial topics. Then phase two be addressed as a whole versus multiple iterations. This is because we feel that multiple iterations will only increase the overall administrative burden on the drafting team, increase complexity of an already complex task, possibly result in throw away work, and impact our ability to deliver a cohesive, quality, and timely product.
<p><b>Response:</b> The SDT is best positioned to determine if a multi-phased approach is appropriate and if yes the timing and grouping of revisions to be</p>		

## Consideration of Comments on 1st Draft of SAR to Revise Cyber Security Standards — Project 2008-06

Organization	Question 4:	Question 4 Comments:
		submitted to the industry for comment and ballot. The multi-phased approach is an option (not a requirement). Should the SDT deem another approach to be superior it has the latitude to proceed as such.
NPCC	No	While we support this as a general approach when NERC develops several standards at the same time, we are unable to further comment on its merit absent any proposed implementation plan and any indication in the SAR as to which standards are "low fruit dropping" and which ones are more controversial than the others. We would suggest, however, that the inter-relationship among these standards be considered in developing the staged implementation plan. We recommend that the SAR be broken into two or more SARs. The first SAR can address the "low hanging," less contentious issues. A second SAR can address the more contentious issues.
		<b>Response:</b> The SDT is best positioned to determine if a multi-phased approach is appropriate and if yes the timing and grouping of revisions to be submitted to the industry for comment and ballot. The multi-phased approach is an option (not a requirement). Should the SDT deem another approach to be superior it has the latitude to proceed as such.
Midwest ISO	No	Registered entities have already been working towards compliance with the CIP standards per the existing implementation plan. Now, this drafting team is proposing to make changes before the existing implementation plan is complete. Registered entities need to be allowed to become compliant to the existing standards. Afterward, then additional changes can be made to the CIP standards. Otherwise, the drafting team is creating a moving target that provides an incentive to delay implementation right up until an entity is required to be auditably compliant. By delaying their implementation, registered entities could save costs from having to make multiple changes to meet changing CIP requirements without incurring penalties. FERC confirmed in order 706 that no penalties could be applied until the auditably compliant phase. We also believe that the drafting team should list the required changes from FERC Order 706 directly in the SAR and what class they consider the change to be in (i.e. low hanging fruit ,etc.) Also, if additional acceptable changes are requested from the commenters, these changes should be listed in the SAR and clearly marked as coming from industry.
		<b>Response:</b> The SDT is best positioned to determine if a multi-phased approach is appropriate and if yes the timing and grouping of revisions to be submitted to the industry for comment and ballot. The multi-phased approach is an option (not a requirement). Should the SDT deem another approach to be superior it has the latitude to proceed as such.
Duke Energy	No	We are concerned about how "easy" versus "contentious" issues will be identified. Furthermore a staggered approach will add complexity to corresponding changes that must be made to the implementation plan. The SDT should consider getting all changes in one revision to simplify the process.
		<b>Response:</b> The SDT is best positioned to determine if a multi-phased approach is appropriate and if yes the timing and grouping of revisions to be submitted to the industry for comment and ballot. The multi-phased approach is an option (not a requirement). Should the SDT deem another approach to be superior it has the latitude to proceed as such.
Ontario IESO	No	We do not agree with the "multi-phase" approach. Such an approach brings out multiple concerns - which set of standards should we begin to focus our attention on while developing implementation plans as these cannot be

Consideration of Comments on 1st Draft of SAR to Revise Cyber Security Standards — Project 2008-06

Organization	Question 4:	Question 4 Comments:
		<p>developed and implemented overnight - what if we or any other applicable entity begin work on a set of standards which ultimately gets voted down by the industry - should we wait to see which set of standards gets the assent which would mean delays in the implementation phases - what factors decide which set of standards go through - would this not bring into the forefront issues related to costs and risk mitigation. There are too many questions that would remain if such an approach were to be applied. We strongly suggest that all these standards be developed and implemented at the same time to avoid confusion. If it becomes necessary to implement these standards in stages, we urge the SDT to consider the inter-relationship among these standards and clearly convey the rationale for a staged implementation plan.</p>
<p><b>Response:</b> The SDT is best positioned to determine if a multi-phased approach is appropriate and if yes the timing and grouping of revisions to be submitted to the industry for comment and ballot. The multi-phased approach is an option (not a requirement). Should the SDT deem another approach to be superior it has the latitude to proceed as such.</p>		
FirstEnergy Corp.	Yes	<p>Regarding the "multi-phase" approach and going after the "low hanging fruit" first, while that may be prudent, it is also important to quickly focus on modifications to CIP-002 since it drives all other CIP requirements. Also, by changing CIP-002 first, the "critical asset list" will be focused solely on whether there is a true belief of BES criticality rather than be influenced by what an organization may have to do to secure the assets. The team should consider three phases: Phase 1: Handle the "urgent" issues for specific changes and timelines as directed by FERC (such as the removal of "reasonable business judgment" phrase from the standards). These could even be handled through separate "Urgent Action" SAR/Standard revisions as allowed by the NERC standard development process. Phase 2: Properly develop CIP-002 since this standard lays the groundwork for the other 7 CIP standards. Phase 3: Develop the rest of the requirements to CIP-003 through CIP-009 per the FERC directed modifications.</p>
<p>The SDT is best positioned to determine if a multi-phased approach is appropriate and if yes the timing and grouping of revisions to be submitted to the industry for comment and ballot. The multi-phased approach is an option (not a requirement). Should the SDT deem another approach to be superior such as your proposed three phases, it has the latitude to proceed as such.</p>		
Hydro One Networks Inc.	No	<p>While this might be an acceptable approach, we are unable to further comment on its merit absent any proposed implementation plan and any indication in the SAR as to which standards are "low hanging fruit" and which ones are more controversial than the others. We would suggest, however, that inter-relationship among these standards be considered in developing the staged implementation plan. Alternatively, the SAR could be broken into several SARs one for each phase.</p>
<p><b>Response:</b> The SDT is best positioned to determine if a multi-phased approach is appropriate and if yes the timing and grouping of revisions to be submitted to the industry for comment and ballot. The multi-phased approach is an option (not a requirement). Should the SDT deem another approach to be superior it has the latitude to proceed as such.</p>		
Southwest Power	No	<p>Comments: We do not agree with the multi-phased approach to implementation. The industry is already</p>

Consideration of Comments on 1st Draft of SAR to Revise Cyber Security Standards — Project 2008-06

Organization	Question 4:	Question 4 Comments:
Pool		implementing the current CIP standards in a phased approach, implementing another series of revised standards in the same manner would only cause confusion as to which standards are applicable when and what is required. This approach also creates an incentive to wait as long a possible to become compliant. If a registered entity commits assets today to become compliant, it may have to commit more later to make modifications to meet the changes to the standards. However, if the registered entity waits until later phases of the implementation plan, it may commit less assets overall since it may avoid multiple investments. As long it complies by the auditably compliant phase, then they cannot be fined for non-compliance, per FERC Order 706.
<p><b>Response:</b> The SDT is best positioned to determine if a multi-phased approach is appropriate and if yes the timing and grouping of revisions to be submitted to the industry for comment and ballot. The multi-phased approach is an option (not a requirement). Should the SDT deem another approach to be superior it has the latitude to proceed as such.</p>		
M-S-R Public Power Agency	No	M-S-R cannot agree with the "multi-phase" approach without knowing how the "easiest modifications" have been or will be identified. If adding PSE to the applicability section of the revised standards has been or could be considered an easy modification, then M-S-R is opposed to the "multi-phase" approach.
<p><b>Response:</b> The SDT is best positioned to determine if a multi-phased approach is appropriate and if yes the timing and grouping of revisions to be submitted to the industry for comment and ballot. The multi-phased approach is an option (not a requirement). Should the SDT deem another approach to be superior it has the latitude to proceed as such.</p>		
WECC (Steve Rueckert)	No	In theory, it is a reasonable approach if the first phase only consist of simple changes to reporting timeframes, etc. that don't have significant interrelation, complexity or controversial topics. Then phase two be addressed as a whole versus multiple iterations. This is because we feel that multiple iterations will only increase the overall administrative burden, increase complexity of an already complex task, possibly result in throw away work, and impact the ability to deliver a cohesive, quality, and timely product
<p><b>Response:</b> The SDT is best positioned to determine if a multi-phased approach is appropriate and if yes the timing and grouping of revisions to be submitted to the industry for comment and ballot. The multi-phased approach is an option (not a requirement). Should the SDT deem another approach to be superior it has the latitude to proceed as such.</p>		
American Transmission Company	Yes	Including a list of all FERC order directives will aid that industry and the SDT to efficiently organize the multiple phases.
<p><b>Response:</b> The SDT is best positioned to determine if a multi-phased approach is appropriate and if yes the timing and grouping of revisions to be submitted to the industry for comment and ballot. The multi-phased approach is an option (not a requirement). Should the SDT deem another approach to be superior it has the latitude to proceed as such.</p>		
American Electric Power	Yes	Logical progression.

Consideration of Comments on 1st Draft of SAR to Revise Cyber Security Standards — Project 2008-06

Organization	Question 4:	Question 4 Comments:
<p><b>Response:</b> The SDT is best positioned to determine if a multi-phased approach is appropriate and if yes the timing and grouping of revisions to be submitted to the industry for comment and ballot. The multi-phased approach is an option (not a requirement). Should the SDT deem another approach to be superior it has the latitude to proceed as such.</p>		
PJM Interconnection	Yes	
Southern Company Services, Inc.	Yes	It is our understanding that the SAR drafting team will consider the directives from the FERC order first and establish a priority level. The less contentious and less complicated items are assumed to be considered first for quick turnaround, followed by the more difficult issues.
<p><b>Response:</b> The SDT is best positioned to determine if a multi-phased approach is appropriate and if yes the timing and grouping of revisions to be submitted to the industry for comment and ballot. The multi-phased approach is an option (not a requirement). Should the SDT deem another approach to be superior it has the latitude to proceed as such.</p>		
AEP	Yes	It should be well established that the standards revisions are not to be construed as standards re-writing. The basic concepts except as noted by FERC in the final rule should stand.
<p><b>Response:</b> The SDT is best positioned to determine if a multi-phased approach is appropriate and if yes the timing and grouping of revisions to be submitted to the industry for comment and ballot. The multi-phased approach is an option (not a requirement). Should the SDT deem another approach to be superior it has the latitude to proceed as such.</p>		
We Energies	Yes	We Energies would like to see the drafting team address modifications as they apply to any requirement(s) throughout the standard set.
<p><b>Response:</b> Note that the Attachment #1 of the SAR includes reviewing each of the standards to ensure that it conforms to the latest version of the ERO Rules of Procedure, including the Reliability Standards Development Procedure as outlined in the Standard Review Guidelines</p>		
Western Electricity Coordinating Council	Yes	This may be more difficult than it seems, but the approach is a good idea and should be allowed. There may be issues that seem easier than others at the onset of the effort which could ultimately end up being far more contentious than originally expected. Greater success may be found if there is a defined process for flexibility around these unforeseen challenges such as a transition mechanism from the "easy" to "hard" range.
<p><b>Response:</b> The SDT is best positioned to determine if a multi-phased approach is appropriate and if yes the timing and grouping of revisions to be submitted to the industry for comment and ballot. The multi-phased approach is an option (not a requirement). Should the SDT deem another approach to be superior it has the latitude to proceed as such.</p>		
ElectriCities of North Carolina, Inc.	Yes	As long as it is perfectly clear to all stakeholders at any time which modifications are under review, which are being balloted, and which are being submitted for approval.
<p><b>Response:</b> The SDT is best positioned to determine if a multi-phased approach is appropriate and if yes the timing and grouping of revisions to be</p>		

Consideration of Comments on 1st Draft of SAR to Revise Cyber Security Standards — Project 2008-06

Organization	Question 4:	Question 4 Comments:
submitted to the industry for comment and ballot. The multi-phased approach is an option (not a requirement). Should the SDT deem another approach to be superior it has the latitude to proceed as such.		
LK4 Technology Corporation	Yes	However, adoption/adaptation of the FFIEC could be a model to speed the phases. The underlying ISO requirements are identical.
<b>Response:</b> The SDT is best positioned to determine if a multi-phased approach is appropriate and if yes the timing and grouping of revisions to be submitted to the industry for comment and ballot. The multi-phased approach is an option (not a requirement). Should the SDT deem another approach to be superior it has the latitude to proceed as such.		
Coral Power, L.L.C.	Yes	
United Illuminating	Yes	
National Institute of Standards and Technology	Yes	
Dominion Resources Services, Inc.	Yes	
Public Service Commission of South Carolina	Yes	
Oncor Electric Delivery Company LLC	Yes	
Electric Power Supply Association	Yes	

## Consideration of Comments on 1st Draft of SAR to Revise Cyber Security Standards — Project 2008-06

5. Based on the limited experience of implementing the current standards, are there any other issues that are not addressed in Order 706 that should be changed?

Summary Consideration: Many commenters identified issues in addition to the directives and recommendations contained in the Order 706. The SAR DT found some to have merit and added these to the SAR as Attachment 3. The additional issues include the following:

- the SDT to develop additional implementation plans as part of their work scope
- address a compliance grace period for assets that are newly identified as critical, acquired through merger/acquisition or other means
- consider the issue of implementing these standards in the substation and generating environment
- consider modifying the standards to clarify the issue of hybrid devices that use both serial and routable protocols
- consider how to provide additional guidance on control centers in support of these standards

Other comments emphasized particular Order 706 directives and recommendations such as coordination with and consideration of other cyber-related standards, guidelines and activities. These items are explicitly listed in the revised SAR, e.g., confer with NRC and others with respect to Nuclear facility exemption.

Organization	Question 5:	Question 5 Comments:
Xcel Energy	Yes	<p>First, we believe that a shift in the approach to development of the CIP standards is needed. We believe that the standards need to be redirected toward performance-based expectations rather than command and control directives. The command and control approach currently embodied in the standards is too rigid and inflexible in a rapidly changing environment to effectively and efficiently protect grid assets from cyber threats that may develop in the coming years. A more performance-based approach would allow industry the flexibility to adjust to a rapidly changing environment in the most efficient and effective manner. In addition, an overall goal or mission statement for the CIP process should be established that clearly identifies the objectives of the standards. Presently, we believe that the distinction between cyber security (which we understand to be the objective of the standards) and physical security is not being effectively maintained in the standards. Clarity about the objective of the CIP standards should help ensure a more clear and precise set of changes to the standards.</p> <p><b>Response:</b> Thank you for the input. The NERC Standards are performance-based as a guiding principle. All standards shall have a clear reliability objective. In Attachment 1 to the SAR, there is an outline of the modifications that will be made to the set of standards, and bringing additional clarity to the requirements is one of the objectives the standard drafting team will try to achieve.</p> <p>With respect to the separation of physical security from cyber security, the family of standards of which these are a part pertain to critical infrastructure protection. These 8 standards pertain to cyber security of which one component is the physical security of those assets.</p>
American	Yes	The SDT should develop a standard timeline for a newly identified Critical Asset to reach compliance. Any newly

**Consideration of Comments on 1st Draft of SAR to Revise Cyber Security Standards — Project 2008-06**

Organization	Question 5:	Question 5 Comments:
Transmission Company		identified Critical Asset will take a considerable amount of time for an entity to become fully compliant with the CIP Standards (CIP-002 - 009). This is not included in the existing CIP standards but we believe that it is something that should be addressed in the phase of standards development. Also, by including a list of all FERC ordered directives in the SAR that SDT will be able to determine when it's best to address these other suggested changes.
<p><b>Response:</b> We agree and thank you for your input. Your suggestion to develop a standard timeline for a newly identified Critical Asset to reach compliance is included in list of added stakeholder issues for the standard drafting team to address. These additional issues are aggregated into Attachment 3 in the revised SAR.</p> <p>A list of the FERC directives has also been added to the revised SAR as Attachment #2.</p>		
PPL Generation, LLC	Yes	The Rev. 1 CIP-007, 008, and 009 standard requirements are largely consistent with the Control Center/SCADA/EMS operating environment. The requirements of these standards are new to generating plant and substation environments. The project should better address the application of CIP-005, CIP-007, CIP-008, and CIP-009 to generation plants and substations, and if appropriate include development of guidance or reference to NIST SP800 series reports.
<p><b>Response:</b> The SAR DT acknowledges that the substation environment is gradually becoming comparable in terms of cyber security importance with control center environments. The following issues have been added to Attachment 3 in the revised SAR:</p> <ol style="list-style-type: none"> <li>1. Consider the unique issues of implementing these standards to the substation and generating environment sub station considerations is among these issues.</li> <li>2. Consider how to provide additional guidance on control centers in support of these standards.</li> </ol>		
Pacific Gas and Electric Company	Yes	In general the industry seems to still be challenged in situations where there are hybrid devices that use both serial and routable protocols. An example is where a Critical Cyber Asset is a serial device which is connected directly to a router, thus converting it to a routable protocol. The SAR should include explicitly address these types of situations. We are not recommending that we expand the current CIP scope to include serial devices, but rather explicit guidance.
<p><b>Response:</b> The SAR DT thanks the commenter for the input. The SAR DT has added a list of stakeholder issues for the standard drafting team to address – and hybrid devices is among those issues. The following issue has been added to Attachment 3 in the revised SAR:</p> <ul style="list-style-type: none"> <li>▪ Consider modifying the standard to clarify the issue of hybrid devices that use both serial and routable protocols.</li> </ul>		
National Institute of Standards and Technology	Yes	General Comments Summary:  NIST believes that if the changes specified in FERC Order 706 and the recommendations below are implemented, NERC will have made a positive step towards making the CIPs commensurate with the NIST SP

Consideration of Comments on 1st Draft of SAR to Revise Cyber Security Standards — Project 2008-06

Organization	Question 5:	Question 5 Comments:
		<p>800-53, Rev 2 moderate baseline. However, there are still differences in coverage and in the level of specificity of the security requirements that need to be addressed. NIST would also like to point out that many of the federal agencies that own/operate industrial control systems in the bulk electric sector are classifying their systems as High impact systems that implement the High baseline requirements in SP 800-53. NIST is willing and has the resources to work on the NERC standards team in developing the next revision to the standard.</p> <p>Approach: Critical Assets vs. Information System - NIST understands that in the electric sector, protecting critical assets has been the predominant paradigm, but recommends for future revisions of the standards that an information systems approach rather than critical asset approach be considered.</p> <p>Our rationale for this suggestion is as follows: While it is important to identify critical assets using a risk-based assessment methodology, NIST suggests that NERC consider applicability of the CIPs at an information system level rather than at the critical asset level. An information system view provides a more <u>natural</u> context for the application of information technology security across an industrial control system composed of multiple components, where some subset of the components is supported by information technology.</p> <p>Under the current scope of the CIPs, all of the CIP security requirements would be applied to every critical cyber asset. In some cases, application of all of the CIP security requirements to a critical cyber asset may not make sense or may be excessive due to the nature of the asset. When an information system view is adopted, the CIP security requirements would be applied at the information system level, resulting in the allocation of CIP requirements to specific components. All components of the information system are not required to support every information system security requirement? just those that are identified as a result of the requirement allocations; thus resulting in significant cost savings.</p> <p>Using the information system view, there is no need to distinguish between cyber assets and critical cyber assets as all cyber assets within the information system are protected. Comments on Specific Requirements</p> <p>CIP 002 R3.1 NIST strongly recommends that a clear unambiguous definition of “routable protocol” be developed and, based on that definition, all routable protocols currently within the scope of the CIPs should be identified. All data encapsulated within a routable protocol should also be within the scope of the CIPs.</p> <p>CIP 002 R3.2 NIST recommends that “control center” should be replaced by “electronic security perimeter.”</p> <p>Nuclear Facility Exemption - In reference to section 4.2.1 of each CIP, NIST observes that the electric side of nuclear power plants can have an impact on the bulk electric sector. NIST suggests that the continuity of power aspects of nuclear facilities should be included in the scope of these standards. Therefore NIST recommends</p>

Consideration of Comments on 1st Draft of SAR to Revise Cyber Security Standards — Project 2008-06

Organization	Question 5:	Question 5 Comments:
		<p>that the exemption statement:                      “Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission be changed to - Specific systems that are regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission (e.g., safety systems).”</p> <p>Wireless - NIST observes that the CIPs do not sufficiently address the security of wireless technologies, which include, but are not limited to, microwave, satellite, packet radio (UHF/VHF), 802.11x, and Bluetooth. There appears to be an assumption in the CIPs that communication occurs solely over media. Consequently, NIST recommends that a clear, unambiguous definition of wireless technology be developed and security requirements for wireless technologies be included in the CIPs.</p> <p>Media Protection - NIST recommends that the CIPs? media protection requirements be expanded to cover all types of media. Because of the miniaturization and increased portability of digital media, protection of this media by a physical security perimeter is no longer adequate. Information system media includes both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks, digital video disks) and non-digital media (e.g., paper, microfilm). Information system media are also components of portable and mobile computing and communications devices (e.g., notebook computers, personal digital assistants, cellular telephones). The organization should have policy and procedures to protect and control information system media during transport outside the physical perimeter and restrict the activities associated with transport of such media to authorized personnel. For example, many organizations today prohibit removing laptop computers with unencrypted hard drives from the physical protection perimeter, and enforce this policy with unannounced inspection at the exits. Information system media is also a component of telephone systems that have the capability to store information (e.g., voicemail systems). Since telephone systems do not have, in most cases, the identification, authentication, and access control mechanisms typically employed in other information systems, policy should address the types of information stored on telephone voicemail systems that are accessible outside of physically protected areas.</p>
<p><b>Response:</b></p> <ul style="list-style-type: none"> <li>• Re Approach: “Critical Assets vs. Information Systems” – Control systems are specialized types of information systems. Accordingly, the SAR DT finds merit in this recommendation, particularly concerning data and control system operations centers. On the other hand, while substation and generation site networked-computing is growing more sophisticated, and at the same time general purpose information systems technology is being more widely employed. These operating environments are quite different than that of data and control system operations centers, and have a number of unique considerations. The SDT may consider splitting the CIP Standards requirements to address each of these two different operating environments. It may be appropriate to use “Information System” oriented thinking for data and control system operation centers, and “Critical Asset” oriented thinking for field and generation environs, at least until more mainstream networked “Information Systems” technology is</li> </ul>		

**Consideration of Comments on 1st Draft of SAR to Revise Cyber Security Standards — Project 2008-06**

Organization	Question 5:	Question 5 Comments:
		<p>more widely applied in those settings. The SAR DT does believe that a programmatic approach to control system cyber security is necessary. That is, control systems are just that – systems – and both control system components individually, and their working together in unison as an operational control system must be properly secured in a systematic manner. Per FERC Ruling 706, the SDT must consider adaptation of the NIST Security Risk Management Framework for electric sector control systems, and it would appear prudent to also consult similar bodies of work such as ISO/IEC 27001 and ISA99 as cross-checking resources to assure thorough and qualitative coverage of the issues. The SAR DT directs that this NIST recommendation be earnestly considered, regardless of whether or not the noted bifurcated approach described above is employed.</p> <ul style="list-style-type: none"> <li>• Re Comments on Specific Requirements:               <ol style="list-style-type: none"> <li>(1) Routable protocols: The SAR DT does not understand the intent and meaning of this comment. Use of “routable protocols” in original CIP drafting was intended in practical terms to refer to movement of data between and through subnetworks using IP datagrams employing a native addressing paradigm; this was specified as such generically due to the potential for other protocols with equivalent functionality to be used or emerge at a later date. Without further clarification from NIST, the SAR DT is unable to reply to this comment further, except to note that the entire discussion may be moot. Based upon the language of FERC Ruling 706, it may be at some point required that all control system critical cyber asset data communications must be secured regardless of protocol or media. Further clarification and discussion as to FERC’s intent in its Directed Modifications will likely be necessary before the SDT can productively engage on this topic.</li> <li>(2) Re protection of encapsulated data: Relevant data or information must be appropriately protected regardless of state, i.e., in storage, being transmitted, or being processed. Communications transmission of critical cyber asset data/information must be protected regardless of media being employed, e.g., copper, glass, air. Also see the comment-reply below concerning media.</li> <li>(3) Re “Control Center”: It is acknowledged that this term is a traditional colloquialism originating from the days when EMS/SCADA operator consoles and the control systems to which they were connected typically were geographically collocated. This obviously need not be the case today or in the future. The SDT will have to alternatively employ more appropriate terminology in the CIP update process.</li> </ol> </li> <li>• Re Nuclear Facility Exemption: It is necessary to obtain further clarification as to the respective roles and responsibilities of Nuclear Plant Operators and Transmission Operators concerning the switchyard interface, and even potentially concerning assets within the nuclear plants themselves, e.g., non-safety systems components. Direct interaction between the SDT and NRC/CNSC ultimately may be needed to attain needed clarity as to respective scope of oversight responsibilities. A formal memorandum of understanding in some form also may be appropriate. The SDT will have to embrace the matter accordingly.</li> <li>• Re Wireless: The Standards do not preclude wireless as a medium and the SAR DT recommends the SDT provide any necessary clarification during the drafting phase.</li> <li>• Re Media Type: “NIST recommends that the CIPs media protection requirements be expanded to cover all types of media.” The SAR DT agrees and directs attention to CIP-003, R4.1, which states: “The Critical Cyber Asset information to be protected shall include, at a minimum and regardless of media type... “IAs NIST observes, there is a wide variety of media that can be employed, and each type should be evaluated for</li> </ul>

**Consideration of Comments on 1st Draft of SAR to Revise Cyber Security Standards — Project 2008-06**

Organization	Question 5:	Question 5 Comments:
		<p>special considerations that may warrant explicit or additional treatment in the Standards' language. NIST's observation about voice mail systems is instructive as an example of the far ranging scope of considerations that have CIP significance, to wit, recordings of operator and/ or systems administrator interactions during a cyber security incident. Yet at the same time, it must be acknowledged that the media here is merely another instance of magnetic tape or disk storage. Finally, similar to the comment-reply under "wireless" above, detailed treatment of all manifestation of different storage media alternatives within the body of a Standard may not be appropriate, and might be better addressed in Supplemental Guidance or Guidelines. The SDT will have to weigh the alternative approaches in drafting.</p> <ul style="list-style-type: none"> <li>In regard to participation on drafting phase, the SAR DT thanks you for your interest. The Standards Committee will solicit Standard Drafting team nominations and appoint them in accordance with segment representation and geographical diversity. Please look for the opening of nomination period on the NERC web pages. While not all nominations can be accommodated, interested persons are welcome and encouraged to remain engaged in the process. All drafting team meetings are open to all interested parties.</li> </ul>
We Energies	Yes	<p>Compliance dates for any additional critical assets that need to be included as a result of the revised standards, or any new requirements for existing critical assets will require extended dates for compliance. The FERC 706 order will create changes in the NERC CIP requirements that will most likely be approved after some of the existing compliance dates have passed.</p>
<p><b>Response:</b> We agree and thank you for your input. Your suggestion to address additional implementation plans and a compliance period for assets that are newly identified as critical, acquired through merger/acquisition or other means are included in a list of new stakeholder issues for the standard drafting team to address - these issues are in Attachment 3 of the revised SAR.</p>		
NPCC	Yes	<p>We do not want to limit the SAR to 706. We suggest that:</p> <ol style="list-style-type: none"> <li>1) the inclusion/exclusion of Generation should be clarified</li> <li>2) either delete CIP-001 or add it to CIP-008</li> <li>3) add the definition of a control center</li> <li>4) clarify that if a control center has a backup that demonstrates the control center's criticality, then the control center should be considered a Critical Asset</li> </ol>
<p><b>Response:</b> Thank you for your input.</p> <ol style="list-style-type: none"> <li>1. The standard drafting team is tasked with improving the clarity in the standards as part of the revision work scope. As a supplement to aid in understanding the current CIP standards, the CIPC Risk Assessment Working Group is drafting guidance for use by the industry. This guidance will be posted for public comment and the SAR DT respectfully invites the commenter to review the guideline as it becomes available.</li> <li>2. CIP-001 is not included in the scope of this project. The CIPC issued a recent guideline entitled, "Threat and Incident Reporting" wherein it aggregates reporting needs of NERC, DOE, ES-ISAC, DHS and RCMP. This guideline may found at <a href="http://www.esisac.com">www.esisac.com</a>.</li> <li>3. The standard drafting team is tasked with improving the clarity in the standards as part of the revision work scope. Definitions are included in that work scope especially when a word or phrase is used in specific sense and/or context. As a supplement to aid in</li> </ol>		

Consideration of Comments on 1st Draft of SAR to Revise Cyber Security Standards — Project 2008-06

Organization	Question 5:	Question 5 Comments:
		<p>understanding the current CIP standards, the CIPC Risk Assessment Working Group (RAWG) is drafting guidance for use by the industry. A definition of control center is anticipated in that guidance. This guidance will be posted for public comment and the SAR DT respectfully invites the commenter to review the guideline as it becomes available.</p> <p>4. Clarification of the criteria used in determining which cyber assets are critical cyber assets is included in the RAWG guidance, and is part of the clarity improvement work scope of the drafting team.</p>
Southern Company Services, Inc.	Yes	<p>For the future, implementation plan(s) should be reviewed to determine overlapping and interrelated issues of timing and revised appropriately (e.g. CIP-004, CIP-005 &amp; CIP-006 may need to have requirements listed in better order so that background checks and training is done ?after? the electronic and physical perimeters are defined).Need flexibility to apply emerging technologies that improve the reliability of the bulk electric system rather than reducing reliability just to comply with the CIP standards.</p> <p>Need more granularities to the term ?critical?. There are indeed levels of criticality but these are not captured in the current standards. In much of the comments concerning NERC’s CIP standards, one of the main objections raised is the great degree of flexibility in determining what assets are within scope. However from a utility viewpoint, the main issue with the NERC CIP standards is actually their inflexibility. With all the talk of choosing our own assets using “risk based methodologies”, ?reasonable business judgment?, ?technical exceptions?, and ?acceptance of risk? it may be surprising to hear that anyone feels the standards are inflexible. However, the CIP-003 to CIP-009 standards are clearly written to apply to control room data centers and the types of cyber assets contained within them. These standards, which are appropriate for that environment, are then broadly applied to assets in the field such as substations and plants. The standards are inflexible in that they require this data-center like security around assets that are located in environments that are nothing like a data center. This base tension between data center environments and field environments is the reason that such flexibility must be included in CIP-002 and then sprinkled throughout the others. The issue with CIP-002 is actually in the inflexibility of CIP-003 to CIP-009. If the standard and its existing requirements were to be scoped to data-center environments for control systems, the standard would need much less flexibility throughout. A separate set of standards could then be developed through the NERC process that is more appropriate for assets located in the field. But with a scope of ?anything with a chip in it located anywhere in your service territory? then much flexibility is required. The CIP-002 standard only allows two classes of assets ? a cyber asset is either ?critical? and is to be protected to data-center level security or its ?not-critical? and is out of scope. The standard allows no middle ground, no ?risk based? protection, absolutely no flexibility in protecting those assets that fall somewhere in-between. It is purely binary. It is analogous to writing security standards appropriate for the cash processing operations of the central Federal Reserve banks that handle massive amounts of cash and then forcing them to apply to every location which houses any cash whatsoever, including all ATMs located in the field. The cost is prohibitive, you actually hinder the legitimate use of the asset, and the decrease in risk for the majority of the assets covered is negligible. For the most part, this tension revolves around the physical security and</p>

**Consideration of Comments on 1st Draft of SAR to Revise Cyber Security Standards — Project 2008-06**

Organization	Question 5:	Question 5 Comments:
		<p>personnel aspects of the standard and their implementation for field locations. The standards go outside of typical technical, electronic access cyber security issues and enforce physical security and personnel-oriented security issues in a cyber asset focused vacuum. One cannot look at personnel or physical security issues holistically even on a site basis; no it must be focused solely on a particular cyber asset. This forces the industry to do costly things that bring little to no benefit or risk reduction and waste resources solely to be compliant to an inflexible standard that could be better spent reducing larger security vulnerabilities elsewhere. This is what causes most of the consternation and the desire to maintain great degrees of flexibility and control scopes within these standards.</p>
<p><b>Response:</b> The SAR DT agrees with your suggestions to address additional implementation plans, consider the unique issues of implementing these standards to the substation and generating environment and to consider how to provide additional guidance in support of these standards. These have been included on a list of added stakeholder issues for the standard drafting team to address. These additional issues are in Attachment 3 of the revised SAR.</p> <p>With respect to defining additional gradation of critical assets, any added distinction made among critical assets may result in not protecting “lower level critical assets” in favor of the higher. It adds a level of complexity.</p> <p>In regard to emerging technologies, the standards do not preclude them nor prohibit their application.</p> <p>The standard drafting team is tasked with improving the clarity in the standards as part of the revision work scope. As a supplement to aid in understanding the current CIP standards, the CIPC Risk Assessment Working Group is drafting guidance for use by the industry. This guidance will be posted for public comment and the SAR DT respectfully invites the commenter to review the guideline as it becomes available.</p> <p>While direction from FERC on the removal of “reasonable business judgment” and “acceptance of risk” will limit the amount of flexibility within the scope of the Standards, the drafting team must address these items mandated by FERC to be removed and the additional direction to narrowly define technical feasibility.</p> <p>Of the 8 standards that pertain to cyber security, including one which covers physical security of those cyber assets the “bar is set” by these standards. An entity may choose to exceed the standards. However at present there are no NERC reliability standards for the physical security of critical assets.</p>		
Western Electricity Coordinating Council	Yes	<p>WECC would like to see additional clarity around CIP-003-01.R3, specifically with respect to the difference between exception to policy and exception based on technical feasibility. Additionally, any potential situations other than technical feasibility which may commonly warrant exception should also be clarified within this effort. WECC agrees with FERC and the Blackout Report (FERC CIP NOPR, paragraph 139) that inappropriate disclosure of information should be prevented. This matter could be clarified by improving the language in CIP-</p>

**Consideration of Comments on 1st Draft of SAR to Revise Cyber Security Standards — Project 2008-06**

Organization	Question 5:	Question 5 Comments:
		003-01.R4 to describe the type of "protection" required. For example, language around digital protection such as encryption (at rest and in transit) for data elements and physical protections such as locked storage for maps, diagrams and other printed materials could be added. Additionally, verbiage describing if/how the information relevant to CIP-003-01.R4 is/isn't "data" that should be classified as a Critical Cyber Asset per the definition(s) provided in the NERC Glossary would be beneficial. Based on feedback from Registered Entities, there appears to be some confusion around how the requirements within CIP-005-01.R1.3 and CIP-006-01.R1.1 relate to one another. The crux of the issue is whether or not an entity can create one large Electronic Security Perimeter using Virtual Private Network (VPN) or similar technology to act as a "conduit" between physical facilities, or if they should maintain an individual Electronic Security Perimeter at each physical facility within a Physical Security Perimeter. WECC requests additions to the relevant CIP standards providing sufficient direction in this area.
<p><b>Response:</b> The SDT will address this issue as identified in Order 706 p.186 specifically the narrowing of the definition for "Technical Feasibility Exceptions".</p> <p>The SAR DT agrees with your suggestions to consider the issue of data versus information protection and to develop a guideline document to address extended LANs over multiple geographically dispersed locations. These suggestions have been added to the list of Stakeholder Issues in Attachment 3 of the revised SAR..</p>		
Ohio Valley Electric Corporation	Yes	How do the standards apply when a new Critical Cyber Asset is deployed? Is there a grace period to bring it into compliance? The drafting team should address this issue.
<p><b>Response:</b> We agree and thank you for your input. Your suggestion to address additional implementation plans and a compliance grace period for assets that are newly identified as critical, acquired through merger/acquisition or other means has been added to the list of Stakeholder Issues in Attachment 3 of the revised SAR..</p>		
Midwest ISO	Yes	How do the standards apply when a new Critical Cyber Asset is deployed? Is there a grace period to bring it into compliance? The drafting team should address this issue.
<p><b>Response:</b> We agree and thank you for your input. Your suggestion to address additional implementation plans and a compliance grace period for assets that are newly identified as critical, acquired through merger/acquisition or other means has been added to the list of Stakeholder Issues in Attachment 3 of the revised SAR..</p>		
LK4 Technology Corporation	Yes	Proof of policy relating to risk assessment produces "Auditable Compliance". This was the standard adopted decades ago by the National Security Agency and then NIST.
<p><b>Response:</b> Thank you for your comment and input.</p>		
WECC-NERC PMO - PacifiCorp	Yes	The order as written does not adequately address the common security practice of using site-to-site VPN technologies to extend a trusted security zone across multiple locations. With respect to the CIPRS, where the

Consideration of Comments on 1st Draft of SAR to Revise Cyber Security Standards — Project 2008-06

Organization	Question 5:	Question 5 Comments:
		VPN endpoints are under the sole control of and within the Physical Security Perimeters of the same responsible entity, a properly configured VPN should be considered adequate mitigation of physical attacks against the communications link.
<p><b>Response:</b> The SAR DT recommends that the SDT consider developing a guideline document to address extended LANs over multiple geographically dispersed locations. This has been added to the list of Stakeholder Issues in Attachment 3 of the revised SAR.</p>		
Hydro One Networks Inc.	Yes	There is now an opportunity to extend the SAR's scope beyond the content in the FERC Order, provided that FERC timelines can still be met. Interpretations which were made subsequent to the standards should be formally codified into the appropriate places in the standards, such as the CIP-006 interpretation. Similarly, experience from entities implementing the Cyber Standards should be taken into consideration as there have been valuable lessons learned.
<p><b>Response:</b> Thank you for your input. These additional stakeholder issues are included in Attachment 3 of the revised SAR. Revisions will incorporate the clarifications from the Interpretation of CIP-006-1 Requirement 1.1.</p>		
FirstEnergy Corp.	Yes	Although the Order discusses contractors and vendors, the standards may need more clarity with regard to how far a responsible entity must go to assure matters such as background checks are properly completed. The team should consider adding to the Scope of the SAR: "With regard to third-party vendors and contractors, provide clarification and additional guidance as to how much a responsible entity may rely on the processes and procedures of contractors and vendors that support the critical infrastructure of that responsible entity under the CIP standards and still be compliant with the standard."
<p><b>Response:</b> The SAR DT has added your suggestion to Attachment 3 of the revised SAR.</p>		
WECC (Steve Rueckert)	Yes	SAR should include an item that CIP2-9 explicitly addresses serial devices as the industry seems to be challenged in situations where there are hybrid devices that use both serial and routable protocols. An example is where a Critical Cyber Asset is a serial device connected directly to a router, thus converting it to a routable protocol. This is not a recommendation that the CIP2-9 scope be expanded to include serial devices, but that CIP2-9 provide explicit guidance.
<p><b>Response:</b> The SAR DT thanks the commenter for the input. Your suggestion to consider modifying the standard to clarify the issue with respect to hybrid devices that use both serial and routable has been added to the list of Stakeholder Issues in Attachment 3 of the revised SAR.</p>		
Southwest Power Pool	Yes	Comments: The four tables in the Implementation Plan prescribe the initial compliance schedule for a registered entity, with Table 4 addressing new entities that register in the future. But there is no table prescribing a schedule in which an existing registered entity can bring a newly identified critical asset and its critical cyber assets into compliance. While not expected to change frequently, the critical asset list can change for any number of valid reasons (including new guidance from FERC, NERC or the Regional Entities as to what constitutes a "critical asset" for purposes of the CIP Standards), and the registered entity needs to have an appropriate period of time

**Consideration of Comments on 1st Draft of SAR to Revise Cyber Security Standards — Project 2008-06**

Organization	Question 5:	Question 5 Comments:
		in which to achieve compliance with the standards for that asset. In the absence of a compliance schedule, no guidance is available to either the registered entity or the auditor. A new table should be developed defining a compliance schedule for standards CIP-003 through CIP-009 applicable to newly identified critical assets and based upon the date of the risk assessment. The new table should give due consideration to those CIP requirements that are broadly applicable to the entity and should already be in compliance, and those requirements that require new resources and effort and should be afforded adequate time to reach compliance. That consideration should include consideration whether or not the entity had previously identified any critical assets.
<p><b>Response:</b> We agree and thank you for your input. Your suggestion to address additional implementation plans and a compliance grace period for assets that are newly identified as critical, acquired through merger/acquisition or other means has been added to the list of Stakeholder Issues in Attachment 3 of the revised SAR.</p>		
Duke Energy	No	However the House Subcommittee concerns about critical infrastructure protection are not addressed. After implementing FERC's direction the CIP standards will still only cover a small fraction of the assets identified by the House Subcommittee. Because of this, the CIP standards will continue to come under criticism.
<p><b>Response:</b> Thank you for your comment and input. The NERC Reliability Standards are focused upon ensuring reliable operation of the BES as a whole, not the continued operation of an individual asset.</p>		
AEP	No	
Dominion Resources Services, Inc.	No	
ElectriCities of North Carolina, Inc.	No	
Public Service Commission of South Carolina	No	
Oncor Electric Delivery Company LLC	No	
Ontario IESO	No	
Electric Power	No	

Consideration of Comments on 1st Draft of SAR to Revise Cyber Security Standards — Project 2008-06

Organization	Question 5:	Question 5 Comments:
Supply Association		
M-S-R Public Power Agency	No	
American Electric Power	No	
PJM Interconnection	No	
Detroit Edison	No	
Ontario Power Generation	No	
Coral Power, L.L.C.		no comment
United Illuminating	No	

**Consideration of Comments on 1st Draft of SAR to Revise Cyber Security Standards — Project 2008-06**

6. If you have any other comments on this SAR that you haven't already provided in response to the prior five questions, please provide them here.

Summary Consideration: There are several comments encouraging the SDT work with the regional entities and the FERC which are acknowledged and appreciated. The SAR DT disagreed with a commenter's recommendation that Transmission Service Providers not be subject to these CIP Standards. The SAR DT believes that the functions performed by the TSP are essential to real time reliable operation of the BES and therefore should be subject to the CIP Standards. The existing CIP-002-1 through CIP-009-1 already apply to the Transmission Service Provider.

The SAR DT concurs with a commenter with respect to focusing the SDT upon the NIST framework and also agrees that other relevant publications/technical reports such as from the MITRE corporation, the DHS and National Laboratories should also be considered. These have been added to the SAR.

Organization	Question 6 Comments:
XcelEnergy	It is not clear that the current body of CIP standards was based on any real assessment or understanding of potential risks to the bulk electric system of terroristic threats. Rather, it appears that the standards were developed at the micro level based on perceived risks to specific pieces of equipment without a holistic understanding of how grid systems work or where the greatest vulnerabilities really lie. We believe that the next round of CIP standards should be guided by a more clearly defined set of risks which can result in a more focused and effective set of compliance expectations.
<p><b>Response:</b> Thank you for your comment and input. The NERC Reliability Standards are focused upon ensuring reliable operation of the BES from a broad spectrum of threats. The SAR DT has added your suggestion to a list of issues for the standard drafting team to address in Attachment 3 of the revised SAR.</p>	
PJM Interconnection	It is vitally important that NERC and the Regional Entities work together to provide a common set of auditing guidelines so that they may be distributed to the industry to help with compliance efforts. Each Responsible Entity has been left with the task of interpreting the CIP Standard requirements and have no way of telling whether their efforts and opinions are correct. There is a very real and serious concern by the Responsible Entities that they could be found in non-compliance due to a difference in opinion or interpretation of any given CIP Standard requirement. With an aggressive Implementation Schedule, these concerns should be addressed as soon as possible. After the SAR process is completed, the same guidance will need to be developed and produced to the Responsible Entities in the industry.
<p><b>Response:</b> The Compliance Program is currently developing Reliability Standard Audit Worksheets (RSAWs) for the existing CIP Standards. Clarification of the criteria used in determining which cyber assets are critical cyber assets is included in the CIPC Risk Assessment Working Group (RAWG) guidance, and is also part of the drafting team work scope. Improving clarity of the standard requirements is among the standard drafting team's tasks.</p>	

Consideration of Comments on 1st Draft of SAR to Revise Cyber Security Standards — Project 2008-06

Organization	Question 6 Comments:
Pacific Gas and Electric Company	1) Suggest that FERC be an active participant in drafting both the CIP 2-9 SAR and subsequent standards revisions 2) Emphasize the need for the scope of the revisions to CIP002 to address the need for a consistent framework to identify critical assets.
<p><b>Response:</b></p> <ol style="list-style-type: none"> <li>1. The standard development process encourages FERC participation in clarifying the directives in Order 706.</li> <li>2. Clarification of the criteria used in determining which cyber assets are critical cyber assets is included in the CIPC Risk Assessment Working Group (RAWG) guidance, and is part of the clarity improvement work scope of the drafting team.</li> </ol>	
Transmission Agency of Northern California	<p>The Transmission Agency of Northern California (?TANC?) appreciates the opportunity to comment on this SAR. TANC believes that the applicability of the Cyber Security Standards (i.e. CIP-002-1 through CIP-009-1) to Transmission Service Providers (?TSP?) is inappropriate and unnecessarily burdensome on entities registered as TSP, and thereby requests that this applicability be removed in the revised standards. FERC Order 706 conditionally approved the current versions of the Cyber Security Standards and directed modifications to the standards that are initiated by this SAR. In Order 706 at Paragraph 49, FERC cautions against an "overly-expansive" approach "requiring that any entity connected to the Bulk-Power System, regardless of size, must comply with the CIP Reliability Standards irrespective of the NERC registry. "TANC contends that business practices related to the TSP function do not involve any Critical Cyber Assets and therefore concludes that the current TSP applicability of the revised standards is inappropriate. In its "Glossary of Terms Used in Reliability Standards" as adopted by the NERC Board of Trustees on February 12, 2008, NERC provides the following definitions of terms essential to the applicability of the CIP standards: Critical Assets: Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System. Cyber Assets: Programmable electronic devices and communication networks including hardware, software, and data. Critical Cyber Assets: Cyber Assets essential to the reliable operation of Critical Assets. The TSP's primary functions are administering the transmission tariff and processing transmission service requests in accordance with its tariff and transmission service agreements. In this capacity, the TSP calculates Available Transfer Capability, approves transmission service requests from customers, and validates e-tags received from the Interchange Authority for confirmation that the interchange schedule references a valid transmission reservation. Computer systems used by the TSP are limited to the OASIS and e-tagging systems, both of which are typically third-party hosted web-based applications. Many TSPs use a common third-party vendor for these systems. As these systems are typically hosted externally to the TSP, there are no Critical Cyber Assets necessarily owned by the TSP, and applying the CIP standards individually to TSPs imposes unnecessary costs of compliance on these entities. It is also unlikely that degradation of these systems used by the TSP would affect the reliability or operability of the Bulk Electric System because these systems are not involved in actual Bulk Electric System operations. The NERC Functional Model (Version 3) states that the Transmission Service Provider does not itself have a role in maintaining system reliability in real time ? that is the</p>

**Consideration of Comments on 1st Draft of SAR to Revise Cyber Security Standards — Project 2008-06**

Organization	Question 6 Comments:
	<p>Reliability Coordinator's and Transmission Operator's responsibility. The TSP's systems support commercial activities involved in the administration of the transmission tariff and forward planning activities (information related to facility ratings and transfer capabilities) that do not pose the same degree of risk to reliability as systems involved in transmission system operations, monitoring and controls. Continuing to include TSP in the applicability section of the revised standards causes every entity registered as TSP to comply with the requirements of CIP-002 only to annually confirm that they have no Critical Cyber Assets related to that function. Such an exercise would be unnecessarily burdensome to entities that are already incurring high costs to comply with the appropriately applicable standards.</p>
<p><b>Response:</b> The SAR DT thanks the commenter for its input. The team does not agree with the argument of the commenter to remove TSP from applicability of the CIP standards. The Functional Model identifies the following tasks performed by a TSP:</p> <ul style="list-style-type: none"> <li>• TSPs approves or denies transmission service requests from PSEs, GOPs and LSEs.</li> <li>• Confirms transmission service requests to IAs</li> <li>• Provides loss allocation to BAs</li> </ul> <p>The SAR DT believes that these functions are essential to real time reliable operation of the BES and therefore should be subject to the CIP Standards. Note that the existing approved CIP-002-1 through CIP-009-1 all list the Transmission Service Provider as a responsible entity. As the standards are refined, there is an opportunity to look more closely at each of the requirements and, where applicable, to provide greater clarity in identifying the responsible entity. Refer to CIP-002 for criteria to determine critical asset identification.</p>	
NPCC	<p>Of concern is the one size fits all approach by the standards, in that many requirements attempt to address themselves equally to several different cyber environments. NPCC sees major differences with respect to control center environments and configurations, which are more like typical IT Enterprise style environments utilizing readily available hardware, software, and application platforms and processes. Generators, substations, and other small or remote facilities, have older legacy and single function system and process configurations, which can be best described as atypical to control room configurations. The problem lies in the difficulty of trying to define technical requirements that can effectively address the different kinds of cyber environments. The result too often is a requirement that serves no one environment well. The standards attempt to resolve this by leaving it to the Entity to try and figure out what the real requirement is for them, and wondering whether their implementation will be compliant. Therefore NPCC believes that such requirements need to specify which cyber environments they apply to, and ensure they provide appropriate clarity and direction to that environment.</p>
<p><b>Response:</b> The SAR DT acknowledges that the substation environment is gradually becoming comparable in terms of cyber security importance with control center environments. The following issues have been added to Appendix 3 of the revised SAR:</p> <ol style="list-style-type: none"> <li>1. Consider the unique issues of implementing these standards to the substation and generating environment sub station considerations is among these issues.</li> </ol>	

Consideration of Comments on 1st Draft of SAR to Revise Cyber Security Standards — Project 2008-06

Organization	Question 6 Comments:
2. Consider how to provide additional guidance on control centers in support of these standards.	
Southern Company Services, Inc.	We'd ask NERC to consider informing the industry early and often as to the various drafting options you would consider on these CIP standards.
<p><b>Response:</b> The Standard Development Procedure describes the process in detail. It can be found on the NERC website at the following URL: <a href="http://www.nerc.com/standards/newstandardsprocess.html">http://www.nerc.com/standards/newstandardsprocess.html</a></p> <p>Meetings of the SDT and conference calls are open to interested observers with prior notice.</p>	
Western Electricity Coordinating Council	<p>WECC recognizes and supports the shift toward standards that more closely align with the NIST SP800 series. Opportunities during this revision effort should be taken to move the existing CIP standards in that direction. Inclusion of appropriate elements from various Special Publications, and not just SP800-53x, should be considered since there is overlap and interplay between the various SP800 documents. WECC acknowledges the importance of protecting Critical Cyber Assets; however, at some point in time if not part of this revision process, physical security of the Critical Assets must be addressed.</p>
<p><b>Response:</b> There are several documents that have relevance to Cyber Security that have been circulating in industry. A MITRE corporation technical report (MTR070050) analyzes current NERC standards in comparison to NIST SP-800 standard. The MITRE report recommends, "NIST and FERC should work together to develop an interpretation of SP 800-53 that is applicable to both public and private entities in the electric power sector. Another MITRE corporation report offers various approaches to control system security.</p> <p>The National Institute of Standards and Technology has offered its NIST SP 800-53 standard, "Recommended Security Controls for Federal Information Systems" for NERC drafting team consideration and adoption. There is also a Department of Homeland Security report, "Catalog of Control Systems Security: Recommendations for Standards Developers - January 2008" detailing recommendations to increase the security of control systems from both physical and cyber attacks.</p> <p>The SAR DT has explicitly included the Order 706 recommendation to consider features of the NIST framework and other relevant publications/technical reports such as from the MITRE corporation, the DHS and National Laboratories in the revision of the CIP Standards.</p> <p>There are currently no standards for physical security of critical assets however a SAR may be initiated by any stakeholder for the Standards Committee to consider.</p>	
Duke Energy	It appeared that the original drafting team had a strong focus on Energy Management systems supporting Control Centers. When the same CIP standards were applied to Substations, some of the requirements, i.e., patch management, anti virus, etc., had limited applicability. Additional specific expertise is needed on the drafting team to ensure the standards are equally applicable to all relevant Critical Assets. Any changes (particularly in the identification of Critical Assets) MUST include corresponding changes to the implementation plan.

**Consideration of Comments on 1st Draft of SAR to Revise Cyber Security Standards — Project 2008-06**

Organization	Question 6 Comments:
	<p><b>Response:</b> Thank you for your input. Diverse subject matter experts are included on this SAR DT and will be sought for participation on the SDT. Note that the nomination form used to solicit volunteers for this SAR DT specifically mentioned that the Standards Committee was seeking volunteers who have, “Experience developing or implementing cyber security policies and procedures; experience implementing or managing the implementation of the cyber security standards is preferred.”</p>
Ontario IESO	<p>The four tables in the Implementation Plan prescribe the initial compliance schedule for a registered entity, with Table 4 addressing new entities that register in the future. But there is no table prescribing a schedule in which an existing registered entity can bring a newly identified critical asset and its critical cyber assets into compliance. While not expected to change frequently, the critical asset list can change for any number of valid reasons, and the registered entity needs to have an appropriate period of time in which to achieve compliance with the standards for that asset. In the absence of a compliance schedule, no guidance is available to either the registered entity or the auditor. A new table should be developed defining a compliance schedule for standards CIP-003 through CIP-009 applicable to newly identified critical assets and based upon the date of the risk assessment. The new table should give due consideration to those CIP requirements that are broadly applicable to the entity and should already be in compliance, and those requirements that require new resources and effort and should be afforded adequate time to reach compliance. That consideration should include consideration whether or not the entity had previously identified any critical assets. The applicability of the standards should be expanded to include LSEs, which own BES transmission and/or distribution facilities.</p>
	<p><b>Response:</b> We agree and thank you for your input. Note that every standard drafting team is required to post, as part of its work scope, an implementation plan. The SAR DT has added your suggestion of addressing the time needed to become compliant with the standards when an entity has assets that are newly identified as critical, acquired through merger/acquisition or other means, to a list of items for the drafting team to address in Attachment 3 of the revised SAR.</p>
FirstEnergy Corp.	<p>FE provides the following additional comments:</p> <ol style="list-style-type: none"> <li>1. The Scope will understandably address the FERC directed changes from Order 706. However, there may be instances in the Order where FERC believes a comment is valid but did not specifically direct a change but may merit a further look by the CIP drafting team. Also, as the drafting team work is underway, issues may arise and become more evident in the realm of critical infrastructure protection that may show a glaring need for new requirements. We want to assure that the SAR is not overly narrow in scope as to prevent the drafting team from proposing additional requirements that are both needed and sound.</li> <li>2. Implementation - Throughout this development, the team should keep in mind that there is much work underway and completed by responsible entities in preparation for compliance with these standards as written today. Once changes are made, these entities should be given a reasonable amount of time to make any</li> </ol>

**Consideration of Comments on 1st Draft of SAR to Revise Cyber Security Standards — Project 2008-06**

Organization	Question 6 Comments:
	<p>necessary adjustments. Furthermore, any new implementation schedule should start after the current implementation schedule is complete.</p> <p>3. The SAR proposes to address the following NERC "principles": Reliability Principle 4 [Plans for emergency operation and system restoration of interconnected bulk electric systems shall be developed, coordinated, maintained and implemented] and Market Interface Principle 4 [An Organization Standard shall not preclude market solutions to achieving compliance with that standard]. It is not clear why the SAR should specifically address these principles. Are these not general principles applicable to every standard? If not, then why not address the other 6 Reliability principles and other 4 Market Interface principles?</p> <p>4. NERC approved interpretation of CIP-006-1 R1.1, as well as ongoing interpretation development of CIP-006-1 R1.2 and CIP-005-1 Requirement 1 (per NERC project 2007-30) should be incorporated into the scope of the development of these standards. Also, in the SAR under "Industry Need", reference should be made to "CIP-006-1a" which has incorporated the NERC approved interpretation of R1.1 in Appendix 1.</p>
<p><b>Response:</b></p> <ol style="list-style-type: none"> <li>1. The SAR DT asserts that all matters identified in the Order 706 will be addressed. The SAR will define the scope per the Standard Development Procedure.</li> <li>2. The SDT will be making the determinations for appropriate implementation plan in its drafting work.</li> <li>3. Each standard supports at least one reliability principle and complies with all market interface principles.</li> <li>4. As a matter of course, any approved interpretation in force at the time of standard revision work will be incorporated into the revised version.</li> </ol>	
WECC (Steve Rueckert)	<p>1) Suggest that FERC be an active participant in drafting both the CIP 2-9 SAR and subsequent standards revisions if permissible 2) Emphasize the need for the scope of the revisions to CIP002 to address the need for a consistent framework to identify critical assets.</p>
<p><b>Response:</b></p> <ol style="list-style-type: none"> <li>1. The standard development process encourages FERC participation in clarifying its directives.</li> <li>2. Clarification of the criteria used in determining which cyber assets are critical cyber assets is included in the CIPC Risk Assessment Working Group (RAWG) guidance, and is part of the clarity improvement work scope of the drafting team.</li> </ol>	
Southwest Power Pool	<p>There is concern that entities have internal security measures in place that may exceed the CIP requirements. The SAR should include in its scope that the standard clarify measures for compliance will be relegated to the FERC approved requirements and not any internal policies.</p>
<p><b>Response:</b> The SAR DT thanks you for your comment. The SAR DT has added a list of stakeholder issues for the standard drafting team to</p>	

**Consideration of Comments on 1st Draft of SAR to Revise Cyber Security Standards — Project 2008-06**

Organization	Question 6 Comments:
	<p>address – and the issue where an organization has implemented an information security policy and program that includes requirements beyond the NERC CIP requirements is among those issues. The issue will include review of FERC Order 706 paragraph 377 and the pertinent requirements and compliance information of CIP-003 to make it clear that only non-compliance with the NERC CIP requirements will be subject to non-compliance findings. These additional issues are included in Attachment 3 of the revised SAR.</p>
Coral Power, L.L.C.	None
Electric Power Supply Association	no additional comments
M-S-R Public Power Agency	None.