

Comments — Project 2008-06

Background Information:

In Order 706 FERC directed that NERC make significant changes to each of the following Cyber Security standards:

CIP-002-1	Critical Cyber Asset Identification
CIP-003-1	Security Management Controls
CIP-004-1	Personnel & Training
CIP-005-1	Electronic Security Perimeter(s)
CIP-006-1	Physical Security of Critical Cyber Assets
CIP-007-1	Systems Security Management
CIP-008-1	Incident Reporting and Response Planning
CIP-009-1	Recovery Plans for Critical Cyber Assets

A SAR to revise each of these standards has been posted for stakeholder review. The scope of the SAR includes addressing the directives in Order 706. Refer to <http://www.ferc.gov/whats-new/comm-meet/2008/011708/E-2.pdf> for the complete text of the final order.

The SAR proposes expanding the scope of applicable entities to include the Regional Entity and Purchasing-selling Entity. If the Functional Model Work Group implements changes to the Functional Model in response to 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.

In addition, the scope of the SAR includes making revisions to the standards so they conform to the latest approved versions of the Reliability Standards Development Procedure and the ERO Rules of Procedure as outlined in the Standard Review Guidelines identified in Attachment 1 of the SAR.

While the SAR is still under development, stakeholders can identify additional improvements needed in this set of standards.

Please review the SAR and then answer the following questions. Please submit your responses no later than **April 19, 2008**.

If you experience any problems in using this form, please contact Barbara Bogenrief at 609-452-8060.

Questions:

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

Yes

No

Comments:

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?

Yes

No

Comments:

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

Regional Variance:

Business Practice:

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.)

Yes

No

Comments:

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?

Yes

No

Comments:

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.

Individual
Terri Eaton
Xcel Energy
303-273-4878
terri.k.eaton@xcelenergy.com
MRO, SPP, WECC
1 - Transmission Owners, 3 - Load-serving Entities, 5 - Electric Generators, 6 - Electricity Brokers, Aggregators
No
PSEs are involved in scheduling purchase and sales transactions between entities in the wholesale electric market. We are not aware of any activities undertaken by a PSE that could be manipulated from a cyber standpoint and result in compromising the integrity of the bulk electric system. 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.
No
As noted above, we do not believe that any justification has been provided for extending the reach of the CIP standards to PSEs.
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.
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.
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.
Yes
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.
It is not clear that the current body of CIP standards was based on any real assesment 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.
Individual
Todd Thompson
PJM Interconnection
(610) 666-8264
thompt@pjm.com
RFC
2 - RTOs and ISOs
Yes

Yes
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.
Yes
No
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.
Individual
Kent Kujala
Detroit Edison
(313) 235-9428
kujalak@dteenergy.com
RFC
3 - Load-serving Entities, 5 - Electric Generators, 4 - Transmission-dependent Utilities
Yes
Yes
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
No
Group
Ontario Power Generation
Colin Anderson
Ontario Power Generation
5 - Electric Generators
(416) 592-3326
colin.anderson@opg.com
Yes
see comments below
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.

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.
No
Individual
Jason Shaver
American Transmission Company
(262) 506-6885
jshaver@atcllc.com
RFC, MRO
1 - Transmission Owners
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.
Yes
ATC is not aware of any regional or business variance that the SDT should consider.
Yes
Including a list of all FERC order directives will aid that industry and the SDT to efficiently organize the multiple phases.
Yes
The SDT should develop a standard timeline for a newly identified Critical Asset to reach compliance. Any newly 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.
Group
PPL Supply
Annette Bannon
PPL Generation, LLC
5 - Electric Generators, 6 - Electricity Brokers, Aggregators
610-774-2064
ambannon@pplweb.com
Mark Heimbach
Mark Heimbach
PPL EnergyPlus
PPL EnergyPlus
RFC, RFC
6, 6
Mark Heimbach
Mark Heimbach
PPL EnergyPlus
PPL EnergyPlus
MRO, MRO
6, 6
Mark Heimbach
Mark Heimbach
PPL EnergyPlus

PPL EnergyPlus
NPCC, NPCC
6, 6
Mark Heimbach
Mark Heimbach
PPL EnergyPlus
PPL EnergyPlus
SERC, SERC
6, 6
Mark Heimbach
Mark Heimbach
PPL EnergyPlus
PPL EnergyPlus
SPP, SPP
6, 6
Jim Batug
Jim Batug
PPL Generation
PPL Generation
RFC, RFC
5, 5
Jim Batug
Jim Batug
PPL Generation
PPL Generation
NPCC, NPCC
5, 5
Yes
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.
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.
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.
Group
WECC Critical Infrastructure and Information Management Subcommittee (CIIMS)
Robert Mathews
Pacific Gas and Electric Company
1 - Transmission Owners
(415) 973-0609
rpm4@pge.com

Dave Ambrose
Dave Ambrose
WAPA - Loveland
WAPA - Loveland
WECC, WECC
3, 1, 3, 1
Vern Kissner
Vern Kissner
Tacoma Power
Tacoma Power
WECC, WECC
Marc DeNarie
Marc DeNarie
WAPA - Folsom
WAPA - Folsom
WECC, WECC
3, 1, 3, 1
Jeff Mantong
Jeff Mantong
WAPA - Folsom
WAPA - Folsom
WECC, WECC
3, 1, 3, 1
Gray Wright
Gray Wright
Sierra Pacific Power
Sierra Pacific Power
WECC, WECC
3, 5, 1, 3, 5, 1
Jamey Sample
Jamey Sample
CAISO
CAISO
WECC, WECC
2, 2
No
Please see specific items in questions 2, 4, and 5.
No
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 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).
None
None
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 interations. This is because we feel that multiple interations will only increase the oveall 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.
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 explicit address these types of situations. We are not recommending that we expand the current CIP scope to include serial devices, but rather explicit guidance.
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.
Individual
Gerald Freese
American Electric Power
(614) 716-2351
gsfreese@aep.com
ERCOT, RFC, SPP
3 - Load-serving Entities, 5 - Electric Generators, 6 - Electricity Brokers, Aggregators , 1 - Transmission Owners
Yes
Yes
Yes
Logical progression.
No
Individual
Paul Kerr
Coral Power, L.L.C.
(519) 620-7712
paul.kerr@shell.com
SPP, SERC, WECC, RFC, MRO, NPCC, ERCOT
6 - Electricity Brokers, Aggregators
Yes
Assuming the question should read: "Do you agree with the scope of the proposed standards action ?" The 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.
No
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.

Yes
no comment
none
Individual
Eric Olson
Transmission Agency of Northern California
(916) 852-1673
eolson@navigantconsulting.com
WECC
1 - Transmission Owners
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 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.
Individual
Michael Puscas
United Illuminating
(203) 926-5245
michael.puscas@uinet.com
NPCC
1 - Transmission Owners, 3 - Load-serving Entities
Yes

Yes
Yes
No
Group
National Institute of Standards and Technology
Keith Stouffer
National Institute of Standards and Technology
9 - Federal, State, Provincial Regulatory, or other Government Entities
(301) 975-3877
keith.stouffer@nist.gov
Stu Katzke
Stu Katzke
NIST
NIST
NA - Not Applicable, NA - Not Applicable
9, 9
Marshall Abrams
Marshall Abrams
Mitre
Mitre
NA - Not Applicable, NA - Not Applicable
NA, NA
No
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.
Yes
Yes
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 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. 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. 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 natural 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. 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. 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 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. CIP 002 R3.2 NIST recommends that “control center” should be replaced by “electronic security perimeter.” 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 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).” 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. 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.

Individual

Thad Ness

AEP

614-716-2053

tkness@aep.com

ERCOT, RFC, SPP

5 - Electric Generators, 6 - Electricity Brokers, Aggregators , 1 - Transmission Owners, 3 - Load-serving Entities

Yes

No

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.

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.

No

Individual
William Lucas
We Energies
(414) 221-2220
william.lucas@we-energies.com
RFC
3 - Load-serving Entities, 5 - Electric Generators
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.
Yes
We Energies is not aware of any regional or business variance that the standards team should consider.
Yes
We Energies would like to see the drafting team address modifications as they apply to any requirement(s) throughout the standard set.
Yes
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.
Group
NPCC Regional Standards Committee
Lee Pedowicz
NPCC
10 - Regional Reliability Organizations/Regional Entities
212-840-1070
Lpedowicz@npcc.org
Guy Zito
Guy Zito
NPCC
NPCC
NPCC, NPCC
10, 10
Brian Hogue
Brian Hogue
NPCC
NPCC
NPCC, NPCC
10, 10
David Kiguel
David Kiguel
Hydro One
Hydro One
NPCC, NPCC
3, 1, 3, 1
Kathleen Goodman
Kathleen Goodman
ISO New England
ISO New England

NPCC, NPCC
2, 2
Ben Li
Ben Li
Independent Electricity System Operator
Independent Electricity System Operator
NPCC, NPCC
2, 2
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 to the standards, whereas some changes would be reviewed by industry, balloted, and submitted for approval. 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. 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.
No
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. 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. 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.

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 implementaiton 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.
Yes
We do not want to limit the SAR to 706. We suggest that: 1) the inclusion/exclusion of Generation should be clarified 2) either delete CIP-001 or add it to CIP-008 3) add the definition of a control center 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
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.
Group
Southern Company - Transmission
Jim Busbin
Southern Company Services, Inc.
1 - Transmission Owners
(205) 257-6357
jybusbin@southernco.com
J. T. Wood
J. T. Wood
Southern Company Services, Inc.
Southern Company Services, Inc.
SERC, SERC
1, 1
Roman Carter
Roman Carter
Southern Company Services, Inc.
Southern Company Services, Inc.
SERC, SERC
1, 1
Marc Butts
Marc Butts
Southern Company Services, Inc.
Southern Company Services, Inc.
SERC, SERC
1, 1
Jay Cribb
Jay Cribb
Southern Company Services, Inc.
Southern Company Services, Inc.
SERC, SERC
1, 1
Valerie Piazza
Valerie Piazza
Southern Company Services, Inc.
Southern Company Services, Inc.
SERC, SERC
1, 1
Yes
Please see our response to Question #2.
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.
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.

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.
Yes
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 & 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. 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 ATM's 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 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.
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.
Individual
George W. Brady
Ohio Valley Electric Corporation
(740)289-7297
gbrady@ovec.com
RFC
1 - Transmission Owners
No
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 Assests that directly affect the bulk electric system. Subsequently, these entities could not have any Critical Cyber Assets.
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.
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.
Group
Compliance Department
Patrick Miller
Western Electricity Coordinating Council
10 - Regional Reliability Organizations/Regional Entities
(360) 567-4056
pmiller@wecc.biz
Yes
Yes
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.
Yes
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-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.
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.
Individual
Greg Rowland

Duke Energy
(704)382-5348
gdrowland@dukeenergy.com
RFC, SERC
1 - Transmission Owners, 3 - Load-serving Entities, 5 - Electric Generators, 6 - Electricity Brokers, Aggregators
No
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?
Yes
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.
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.
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.
Group
Midwest ISO Standards Collaborators
Jason L. Marshall
Midwest ISO
2 - RTOs and ISOs
317-249-5494
jmarshall@midwestiso.org
Joe Knight
Joe Knight
Great River Energy
Great River Energy
MRO, MRO
1, 1
Kirit Shah
Kirit Shah
Ameren
Ameren
SERC, SERC
1, 1
Joeseeph DePoorter
Joeseeph DePoorter
Madison Gas and Electric Company
Madison Gas and Electric Company
MRO, MRO
6, 3, 4, 5, 6, 3, 4, 5
No
See our answers to the other questions.
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.
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.
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.
Group
Dominion - Electric Market Policy
Louis Slade
Dominion Resources Services, Inc.
3 - Load-serving Entities, 6 - Electricity Brokers, Aggregators , 5 - Electric Generators
(804) 273-2461
louis.slade@dom.com
Harold Adams
Harold Adams
RFC, RFC
3, 5, 6, 3, 5, 6
Jalal Babik
Jalal Babik
SERC, SERC
3, 5, 6, 3, 5, 6
Yes
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.
Yes
No

Individual
Denise Roeder
ElectriCities of North Carolina, Inc.
(919) 760-6255
droeder@electricities.org
SERC
6 - Electricity Brokers, Aggregators , 4 - Transmission-dependent Utilities, 3 - Load-serving Entities
Yes
However, do not agree with expanding the scope of applicability as stated (see response to Q2).
No
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.
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.
No
Group
Public Service Commission of South Carolina
Phil Riley
Public Service Commission of South Carolina
9 - Federal, State, Provincial Regulatory, or other Government Entities
(803) 896-5154
philip.riley@psc.sc.gov
Yes
Yes
Yes
No
Individual
Greg Ward / Steve Martin
Oncor Electric Delivery Company LLC
(214) 743-6862
steve.martin@oncor.com
ERCOT
1 - Transmission Owners
No

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.
Yes
No
Individual
Ron Falsetti
Ontario IESO
(905) 855-6496
ron.falsetti@ieso.ca
NPCC
2 - RTOs and ISOs
No
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. 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 [...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.
No
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 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. 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.
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 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.
No
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.
Individual
Ken Welch
LK4 Technology Corporation
866-586-8732
kw1@lk4technology.com
NA - Not Applicable
Not Applicable
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 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.
Yes
A cybersecurity system is only as strong as its weakest link. Having unaudited systems interfacing with complying systems represents a large identifiable risk.
Yes
However, adoption/adaptation of the FFIEC could be a model to speed the phases. The underlying ISO requirements are identical.
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.
Group
PacifiCorp
WECC-NERC PMO@pacificorp.com
PacifiCorp
1 - Transmission Owners, 3 - Load-serving Entities, 5 - Electric Generators
503.813.5219
WECC-NERCPMO@PacifiCorp.com
WECC, WECC
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.

NIST 800-82, NIST 800-53 and the catalog of control systems Security: Recommended for Standards Developers (Dept of Homeland Security)
Yes
The order as written does not adequately address the common security practice of using ste-to-site VPN technologies to extend a trusted security zone across multiple locations. With respect to the CIPRS, where the 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.
Individual
David Kiguel
Hydro One Networks Inc.
416-345-5313
David.Kiguel@HydroOne.com
NPCC
3 - Load-serving Entities, 1 - Transmission Owners
No
(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. (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.
No
(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 (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. (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 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.
No
While this might be an acceptable approach, we are unable to further comment on its merit absent any proposed implementaiton 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.
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.

Group
FirstEnergy
Sam Ciccone
FirstEnergy Corp.
5 - Electric Generators, 6 - Electricity Brokers, Aggregators , 3 - Load-serving Entities, 1 - Transmission Owners
(330) 252-6383
sciccone@firstenergycorp.com
Terry Malone
Terry Malone
FE
FE
RFC, RFC
Doug Hohlbaugh
Doug Hohlbaugh
FE
FE
RFC, RFC
Dave Folk
Dave Folk
FE
FE
RFC, RFC
Rob Martinko
Rob Martinko
FE
FE
RFC, RFC
Henry Stevens
Henry Stevens
FE
FE
RFC, RFC
No
See our comments to the rest of the comment form, plus the following: 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. 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.
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.
Yes
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

<p>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>Yes</p>
<p>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>
<p>FE provides the following additional comments: 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. 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 necessary adjustments. Furthermore, any new implementation schedule should start after the current implementation schedule is complete. 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? 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>Group</p>
<p>Electric Power Supply Association</p>
<p>Jack Cashin</p>
<p>Electric Power Supply Association</p>
<p>5 - Electric Generators</p>
<p>202-349-0155</p>
<p>jcashin@epsa.org</p>
<p> </p>
<p> </p>
<p>Yes</p>
<p>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>
<p>No</p>
<p>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>
<p>The implementation plan provided to industry is resulting in some confusion and is open to different regional interpretations. Based on the title for Table 3, it should be applicable to Interchange Authorities, Transmission Owners, Generator Owners, Generator Operators and Load-Serving Entities. Based on the title for Table 4, it is applicable to entities that registered in 2007. That leaves open to interpretation, the question of which Table applies to Interchange Authorities, Transmission Owners, Generator Owners, Generator Operators and Load-</p>

Serving Entities registered in 2007. Since Table 4 implementation dates are tied to the registration dates that were normally in the first half of 2007, entities forced to follow Table 4 would normally have 6-12 months less to achieve compliance. It appears that Table 4 was designed intentionally to give new registrants additional time to comply, but that due to the time used for regulatory processes, the result is the opposite. Namely, registrants have less time than otherwise similarly situated entities to comply with the standards. No justification exists for punishing the new registrants. Registered entities within the WECC region have been told that they are required to follow Table 4 if they were registered in 2007, while registered entities in the RFC region were told that if an entity had filed in "early 2007" they could follow Table 3. WECC registered entities were told that if they did not meet the milestone in Table 4 they are encouraged to file mitigation plans. This is an inconsistency across the regions that should be addressed. We recommend that the Standard Drafting Team be asked to remove this differentiation by eliminating Table 4 and, if necessary, expanding the applicability of Table 3 to include those entities registered in 2007.
Yes
No
no additional comments
Individual
Martin R. Hopper
M-S-R Public Power Agency
(408) 615-6677
msradmin@svpower.com
WECC
9 - Federal, State, Provincial Regulatory, or other Government Entities
No
See Question 2 comments.
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-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.
None.
None.
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.
No
None.
Group
WECC - Critical Infrastructure and Information Management Subcommittee (CIIMS)

Robert Mathews - CIIMS Subcommittee Chair
WECC (Steve Rueckert)
10 - Regional Reliability Organizations/Regional Entities
415-973-0609
rpm4@pge.com
No
See specific items in questions 2, 4 & 5
No
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)."
none
none
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
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.
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.
Group
ISO RTO Council Standards Review Committee
Charles Yeung
Southwest Power Pool
2 - RTOs and ISOs
832-724-6142
cyeung@spp.org
Patrick Brown
Patrick Brown
PM
PM
RFC, RFC
2, 2
Jim Castle
Jim Castle
NYISO
NYISO
NPCC, NPCC
2, 2
Ron Falsetti
Ron Falsetti
IESO

IESO
NPCC, NPCC
2, 2
Matt Goldberg
Matt Goldberg
ISO NE
ISO NE
NPCC, NPCC
2, 2
Brent Kingsford
Brent Kingsford
CAISO
CAISO
WECC, WECC
2, 2
Anita Lee
Anita Lee
AESO
AESO
WECC, WECC
2, 2
Steve Myers
Steve Myers
ERCOT
ERCOT
ERCOT, ERCOT
2, 2
Bill Phillips
Bill Phillips
MISO
MISO
RFC, RFC
2, 2
No
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 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.
No
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 Functional Model changes are made (or if changes are made to the Compliance Registration Criteria), please see

<p>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>No</p>
<p>Comments: We do not agree with the multi-phased approach to implementation. The industry is already 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>
<p>Yes</p>
<p>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 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>
<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>Individual</p>
<p>Daniel Hecht</p>
<p>Sempra Energy Trading LLC and Sempra Energy Solutions LLC</p>
<p>(203) 355-5417</p>
<p>dhecht@sempratrading.com</p>
<p>ERCOT, FRCC, RFC, SPP, WECC, NPCC, MRO, SERC</p>
<p>6 - Electricity Brokers, Aggregators</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</p>

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 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.

No

See answer to Question 1