

Comment Report

Project Name: 2016-02 Modifications to CIP Standards SAR June 2016
Comment Period Start Date: 6/1/2016
Comment Period End Date: 6/30/2016
Associated Ballots:

There were 21 sets of responses, including comments from approximately 21 different people from approximately 21 companies representing 8 of the Industry Segments as shown in the table on the following pages.

Questions

1. The CIP SDT revised the SAR based on the comments received in the previous posting as noted above. Do you agree with these revisions to the SAR? If not, please explain why you do not agree, and, if possible, provide specific language revisions that would make it acceptable to you.

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
Duke Energy	Colby Bellville	1,3,5,6	FRCC,RF,SERC	Duke Energy	Doug Hills	Duke Energy	1	RF
					Lee Schuster	Duke Energy	3	FRCC
					Dale Goodwine	Duke Energy	5	SERC
					Greg Cecil	Duke Energy	6	RF
MRO	Emily Rousseau	1,2,3,4,5,6	MRO	MRO-NERC Standards Review Forum (NSRF)	Joe Depoorter	Madison Gas & Electric	3,4,5,6	MRO
					Chuck Lawrence	American Transmission Company	1	MRO
					Chuck Wicklund	Otter Tail Power Company	1,3,5	MRO
					Dave Rudolph	Basin Electric Power Cooperative	1,3,5,6	MRO
					Kayleigh Wilkerson	Lincoln Electric System	1,3,5,6	MRO
					Jodi Jenson	Western Area Power Administration	1,6	MRO
					Larry Heckert	Alliant Energy	4	MRO
					Mahmood Safi	Omaha Public Utility District	1,3,5,6	MRO
					Shannon Weaver	Midwest ISO Inc.	2	MRO
					Mike Brytowski	Great River Energy	1,3,5,6	MRO
					Brad Perrett	Minnesota Power	1,5	MRO
					Scott Nickels	Rochester Public Utilities	4	MRO
					Terry Harbour	MidAmerican Energy Company	1,3,5,6	MRO
Tom Breene	Wisconsin Public Service Corporation	3,4,5,6	MRO					

					Tony Eddleman	Nebraska Public Power District	1,3,5	MRO
					Amy Casucelli	Xcel Energy	1,3,5,6	MRO
BC Hydro and Power Authority	Patricia Robertson	1,2,3,5		BC Hydro	Patricia Robertson	BC Hydro and Power Authority	1	WECC
					Venkataramakrishnan Vinnakota	BC Hydro and Power Authority	2	WECC
					Pat G. Harrington	BC Hydro and Power Authority	3	WECC
					Clement Ma	BC Hydro and Power Authority	5	WECC
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7	NPCC	RSC	Paul Malozewski	Hydro One.	1	NPCC
					Guy Zito	Northeast Power Coordinating Council	NA - Not Applicable	NPCC
					Mark J. Kenny	Eversource Energy	1	NPCC
					Gregory A. Campoli	NY-ISO	2	NPCC
					Randy MacDonald	New Brunswick Power	2	NPCC
					Wayne Sipperly	New York Power Authority	4	NPCC
					David Ramkalawan	Ontario Power Generation	4	NPCC
					Glen Smith	Entergy Services	4	NPCC
					Brian Robinson	Utility Services	5	NPCC
					Bruce Metruck	New York Power Authority	6	NPCC
Alan Adamson	New York State Reliability Council	7	NPCC					

					Edward Bedder	Orange & Rockland Utilities	1	NPCC
					David Burke	UI	3	NPCC
					Michele Tondalo	UI	1	NPCC
					Sylvain Clermont	Hydro Quebec	1	NPCC
					Si Truc Phan	Hydro Quebec	2	NPCC
					Brian Shanahan	National Grid	1	NPCC
					Michael Jones	National Grid	3	NPCC
					Michael Forte	Con-Edison	1	NPCC
					Kelly Silver	Con-Edison	3	NPCC
					Peter Yost	Con-Edison	4	NPCC
					Sean Bodkin	Dominion	4	NPCC
					Silvia Parada Mitchell	NextEra Energy	4	NPCC
					Brian O'Boyle	Con-Edison	5	NPCC
					Kathleen M. Goodman	ISO-NE	2	NPCC
					Helen Lainis	IESO	2	NPCC
					Laura Mcleod	NB Power	1	NPCC
Colorado Springs Utilities	Shannon Fair	1,3,5,6		Colorado Springs Utilities	Kaleb Brimhall	Colorado Springs Utilities	5	WECC
					Charlie Morgan	Colorado Springs Utilities	3	WECC
					Shawna Speer	Colorado Springs Utilities	1	WECC
					Shannon Fair	Colorado Springs Utilities	6	WECC
Southwest Power Pool, Inc. (RTO)	Shannon Mickens	2	SPP RE	SPP Standards Review Group	Shannon Mickens	Southwest Power Pool Inc.	2	SPP RE
					Jason Smith	Southwest Power Pool Inc	2	SPP RE

					Kim VanBrimer	Southwest Power Pool Inc	2	SPP RE
					John Allen	City Utilities of Springfield	1,4	SPP RE
					Mike Buyce	City Utilities of Springfield	1,4	SPP RE
					Paul Mehlhaff	Sunflower Electric Power Corporation	1	SPP RE
					TARA Lightner	Sunflower Electric Power Corporation	1	SPP RE
ACES Power Marketing	Warren Cross	1,3,4,5	MRO,RF,SERC,SPP RE,Texas RE,WECC	ACES Standards Collaborators	Brazos Electric Power Cooperative, Inc.	BREC	1,5	Texas RE
					Western Farmers Electric Cooperative	WFEC	1,5	SPP RE
					Old Dominion Electric Cooperative	ODEC	3,4	SERC
					Golden Spread Electric Cooperative	GSEC	5	SPP RE
					Prairie Power, Inc.	PPI	1,3	SERC
					Arizona Electric Power Cooperative, Inc.	AEPC	1	WECC
					Hoosier Energy Rural Electric Cooperative, Inc.	HE	1	RF

1. The CIP SDT revised the SAR based on the comments received in the previous posting as noted above. Do you agree with these revisions to the SAR? If not, please explain why you do not agree, and, if possible, provide specific language revisions that would make it acceptable to you.

Bob Reynolds - 10

Answer No

Document Name

Comment

The SPP RE respectfully submits the following two comments to the Project 2016-02 Standards Authorization Request: (1) Reference the comments submitted by the SPP Regional Entity (SPP RE) April 2016. In those comments, the SPP RE pointed out that Tie Line and other Transmission line flow meters appear to have been unintentionally excluded from consideration under CIP-002-5.1, Impact Rating Criterion 2.5. This significant issue does not appear to have been included in the revised SAR. The original SPP RE comment is restated here: "Impact Rating Criterion 2.5 excludes consideration of BES Cyber Assets associated with Transmission lines through its use of "operating between 200 kV and 499 kV at a single station or substation" language. In the instance where the tie line or other flow meter is associated with a Transmission Line operated between 200 and 499 KV in a substation that satisfies the qualifications of Impact Rating Criterion 2.5, the meter will be excluded and not be categorized as Medium Impacting. Additionally, some entities are proffering the argument that the flow meter is not a BES Cyber Asset because its loss or misuse will not affect the reliable operation of the Transmission Facilities in the substation where the meter resides, overlooking the impact the loss of meter information may have on Control Center operations including ACE calculation, security-constrained generation dispatch, AGC, and Situational Awareness. An additional Criterion, specific to Transmission line flow meters, may be required to address this issue." (2) The SPP RE notes that the revised SAR still makes no mention of the consideration of submitted and outstanding Requests for Interpretation. NERC staff has stated publicly that the RFIs would be addressed by the Standards Drafting Team. The SPP RE is aware that at least one of the issues discussed in the April 2016 comments to the SAR has been formally submitted as a Request for Interpretation. To fail to consider outstanding RFIs in the course of modifying the CIP Standards under this SAR would be a missed opportunity to address significant confusion regarding the expectations of the Requirements under question.

Likes 0

Dislikes 0

Response

Mike Smith - 1,3,5,6

Answer No

Document Name

Comment

For virtualization, Manitoba Hydro does not agree with NERC prescribing specific system architecture, technologies or designs. SDT should continue to focus on identifying requirements to meet specific objectives for the virtualization.

Manitoba Hydro agrees with adding more CIP V5 requirements exceptions for CIP Exceptional Circumstance.

Likes 0

Dislikes 0

Response

Emily Rousseau - 1,2,3,4,5,6 - MRO, Group Name MRO-NERC Standards Review Forum (NSRF)

Answer No

Document Name

Comment

The NSRF agrees with the drafting team’s addition of “reviewing and addressing the CIP V5 requirements for CIP Exceptional Circumstances exceptions” to the SAR. However, we request clarification on the scope of Guidelines and Technical Basis sections that may be changed with updates to the associated Standards within this project. We believe that addressing all CIP V5 Guidelines and Technical Basis sections within the scope of this revision may make the project unwieldy as it already contains a substantial scope of work to address FERC directives. We suggest that only Guidelines and Technical Basis sections related to standards language updates should be addressed within the scope of this project.

Likes 0

Dislikes 0

Response

Patricia Robertson - 1,2,3,5, Group Name BC Hydro

Answer No

Document Name

Comment

CIP-002-5.1

A) The topic of adverse impact should provide more clarity on the real-time requirement as well.
B) Per Medium Impact criterion 2.3 for generation resources, need further clarity on the extent of planning horizon > 1 year contingencies to consider regarding the determination of BES Adverse Reliability Impacts to a given Interconnection. The Guidelines and Technical basis of CIP-002-5.1 reference as an example, TPL-003 Category C3 contingency system studies but otherwise, there is no lower or upper limit indicated regarding the depth of contingencies to be considered. The limit is currently subjective for Transmission Planners and Planning Coordinators.

Furthermore, per the definition of Adverse Reliability Impact, there is direct reference to impacts on a given Interconnection but it is not clear whether this is only considering inter-tie paths or general BES impacts beyond a specific BES location (i.e. generation plant or substation). The Guidelines and Technical basis state only widespread impacts are to be considered instead of localized impacts but it is not clear what is considered ‘widespread’.

CIP-005-5 The fundamental concepts of the intermediate system are omitted or subjective. The standards should define what the requirements are for this system, whether it is strictly a jump host (not mentioned in the standards) or can have more functionality (i.e. software installed upon it). This should be included in the ‘Network and Externally Accessible Devices’ section.

CIP-005-5/CIP-003-6 A clear exemption is given for low impact systems is given in CIP-003-6 Guidelines and Technical Basis (CIP-006-6 pg 28) “To future-proof the standards, and in order to avoid future technology issues, the definitions specifically exclude “point-to-point communications between intelligent electronic devices that use routable communication protocols for time-sensitive protection or control functions between Transmission station or substation assets containing low impact BES Cyber Systems,” such as IEC 61850 messaging.” The ‘Network and Externally Accessible Device”

section should address this topic for medium impact BCS/BCA as well. These technologies are not limited to low impact systems and guidance should be provided.

CIP-007-5: Regarding security patch applications and cyber vulnerability assessments:

- Certain legacy devices (i.e. HMIs, PLCs, etc.) can be in a “fragile” state and are at high-risk regarding the application of software updates, which include cyber security related updates. There is a demonstrable risk in breaking their functionality which can have an adverse impact on the BES as the only solution is to replace the device entirely or at best, perform a complete reset of the device. This is mainly due to bugs that could be introduced by vendors through their patches (not enough regression testing done by the vendors) and for which even testing prior to implementation in a production environment may not identify all such bugs prior to implementation. Recommend providing guidance around how to handle the application of cyber security patches to these “fragile” devices and to potentially not mandate security patch applications in all cases where there may be demonstrable evidence of adverse BES impact.
- Further guidance is required within the Guidelines and Technical basis on the exact difference between a ‘paper’ exercise cyber vulnerability assessments (CVA) and ‘active’ CVA with respect to Medium Impact facilities and the extent an entity is expected to go to achieve this. It has been communicated by Regional Entities’ audit approach that paper scans must incorporate some active component to pull configuration settings, etc. from a device for analysis. For legacy devices (namely firmware devices), these active component scans can also pose a risk in breaking the functionality of said devices, which can cause adverse impact to the BES. Recommend including guidance around how to handle CVAs pertaining to these firmware devices without potentially breaking their functionality.

Likes 0

Dislikes 0

Response

Chris Mattson - 1,3,4,5,6

Answer

No

Document Name

Comment

Tacoma asks that the SDT consider removing the final two sentences from the last paragraph of CIP-005-5, Guidelines and Technical Basis, Section 4 – Scope and Applicability of the CIP Cyber Security Standards, Requirement R1. These are shown in bold below for identification:

*The standard adds a requirement to detect malicious communications for Control Centers. This is in response to FERC Order No. 706, Paragraphs 496-503, where ESPs are required to have two distinct security measures such that the BES Cyber Systems do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear that this is not simply redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs. **Technologies meeting this requirement include Intrusion Detection or Intrusion Prevention Systems (IDS/IPS) or other forms of deep packet inspection. These technologies go beyond source/destination/port rule sets and thus provide another distinct security measure at the ESP.***

Tacoma is asking the SDT to consider that there are other methods and technologies for detecting malicious traffic in addition to deep packet inspection. This change to the G&TB would make the standard more consistent with the language in FERC Order No. 706, Paragraph 501 which indicates that it is not the commission’s intent to mandate any specific mechanism to be the second security measure. The language from the FERC order is shown below for reference and the pertinent language is shown in bold:

Paragraph 501. In response to SDG&E and Entergy, in stating that the placement of security measures in front of systems provides a layer of protection for those systems, the Commission was not giving priority to “in front” measures. In fact, the Commission acknowledged in the CIP NOPR that defense

*in depth measures are generally integrated within and constitute part of a system or program. In commenting that defense in depth measures may also be effectively placed in front of a system, the Commission intended only to acknowledge that there are multiple ways to implement a defense in depth strategy. **The Commission is not mandating any specific mechanism to be the second security measure. We are also not requiring uniformity of security measures, only that each responsible entity have at least two security measures unless it is not technically feasible to do so.** The revised CIP Reliability Standard should allow enough flexibility for a responsible entity to take into account each site's specific environment. The Commission believes that this, in conjunction with the allowance of technical feasibility exceptions, alleviates FPL Group's concern that the Commission's proposal is a "one size fits all" approach.*

Also, the SDT should clarify CIP-005 R1 Part 1.5 with respect to encrypted communications either in the G&TB or directly within the requirement language. It important that the SDT clarify how to detect malicious communications when the communications includes encrypted information that is not readily decrypted to allow inspection.

Likes 0

Dislikes 0

Response

Maryclaire Yatsko - 1,3,4,5,6 - FRCC

Answer

No

Document Name

Comment

Although Seminole concurs with all items currently listed in the draft Standards Authorization Request, Seminole recommends that additional items should be included in the SAR. Seminole thanks the SAR team for addressing our previous comments, in addition to those of others, related to Exceptional Circumstances and the Guidelines and Technical Basis.

While the changes addressed are necessary to address mandatory requirements from FERC, this SAR does not address the fundamental deficiencies in the current CIP standards. Until these fundamental issues are addressed, the electric sector will continue to struggle implementing the current standard, be faced with inefficiencies in the standard that do not improve cyber and physical security, and have difficulty using new and improved capabilities in a rapidly evolving marketplace.

Seminole recommends adding the following items to the SAR:

1. Update CIP-002 Requirements and the Guidelines and Technical Basis section to clarify the expectations in complying with this standard. Update evidence requirements to make clear the expectations of the standard. Clarify attachment 1 to address V5TAG Lessons Learned and FAQs. Resolve issues in the Guidelines and Technical Basis that are inconsistent with the definition of BES Cyber Asset and BES Cyber System.

2. The SDT will review applicable Standards and Requirements to clarify the SDT's intent for management of shared Facilities when more than one Registered Entity owns Facilities inside a single asset. Interconnections within the BES and with Distribution Providers within a single asset create significant complexity for entities in some regions. This results in a need for a significant number of MOU, CFR, or JRO that both complicates compliance and the audit process.

3. The SDT will review the Measures in the CIP V5 standards and adjust where appropriate to allow an entity that provides evidence consistent with the identified measures to determine compliance if no deficiencies are identified in the provided evidence. This may include modifying measures to match the CIP Version 5 Evidence Request or by clarifying either the measures or Guidelines and Technical basis to clarify intent for adjustment of the evidence request.

Likes 0

Dislikes 0

Response

Julie Hall - 6

Answer

No

Document Name

Comment

Comments: Entergy requests that more detail be provided regarding the actions that will be considered regarding CIP Exceptional Circumstances. Is more specificity regarding what constitutes a CIP Exceptional Circumstance being considered? Is more specificity regarding how to declare and document a CIP Exceptional Circumstance being considered? Will more clarity regarding standards affected by CIP Exceptional Circumstance, including a possible increase of applicable standards, be considered? Some particular questions Entergy has regarding the scope of standards affected by CIP Exceptional Circumstances include:

- CIP-004-5.1 R3 does not include the “except during CIP Exceptional Circumstances” language, yet the Guidelines and Technical Basis section states “Each Responsible Entity shall ensure a personnel risk assessment is performed for all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, prior to their being granted authorized access, except for program specified exceptional circumstances that are approved by the single senior management official or their delegate and impact the reliability of the BES or emergency response.” The language in the Guidelines and Technical Basis seems logical as it may not be feasible to validate PRA’s during a widespread emergency response (i.e. a hurricane) especially when response support is provided by many other companies and/or vendors across the country. It is requested that the “except during CIP Exceptional Circumstances” language be added to the appropriate parts of CIP-004-5.1 R3, particularly CIP-004-5.1 R3 Part 3.5.
- The “except during CIP Exceptional Circumstances” language exists in CIP-006-5 R2 Part 2.1 and Part 2.2 which states that logging and continuous escorting of visitors is not required during CIP Exceptional Circumstances. However, none of the CIP-006-5 R1 parts include the “except during CIP Exceptional Circumstances” language, which in turn requires alerting, monitoring, logging of access approved individuals. This may not be feasible during a widespread event that results in total loss of power at many sites over a widespread geographical area. It is requested that the “except during CIP Exceptional Circumstances” language be added to the appropriate parts of CIP-006-5, particularly R1 to ensure consistency across CIP-006-5.

Likes 0

Dislikes 0

Response

Scott Brame - 3,4,5 - SERC**Answer** No**Document Name****Comment**

The following comments are from my CIP SME.

• Per paragraph 73, "...the Commission concludes that a modification to the Low Impact External Routable Connectivity definition to reflect the commentary in the Guidelines and Technical Basis section of CIP-003-6 is necessary to provide needed clarity to the definition and eliminate ambiguity surrounding the term "direct" as it is used in the proposed definition. Therefore, pursuant to section 215(d) (5) of the FPA, we direct NERC to develop a modification.

This is where I believe FERC's order falls short. Although, the definition for LERC needs to be improved and needs to reflect the commentary in the Guidelines and Technical Basis section of CIP-003-6. In my opinion, the requirements for low impact critical assets is incomplete. It appears like the SDT was rushed to provide requirements for low impact. Although, the SDT included some basic requirements for low impact critical assets they should have also included requirements for malware and virus protections. In addition, there should be requirements for logging and auditing of systems and system access. These requirements do not need to be as stringent and comprehensive as what is required for medium and high impact critical assets, but they should also be required for low impact critical assets.

Likes 0

Dislikes 0

Response**Warren Cross - 1,3,4,5 - MRO,WECC,Texas RE,SERC,SPP RE,RF, Group Name** ACES Standards Collaborators**Answer** No**Document Name****Comment**

Thank you for the opportunity to provide comments regarding the Standards Authorization Request (SAR) in response to FERC Directives and v5TAG recommendations. While the current SAR attempts to resolve issues around LERC, virtualization and communication protections, ACES believes the SAR doesn't adequately detail the areas of concern for LERC and fails to allow for technology advances, which may ultimately hinder industry adoption of more secure solutions to address cyber security threats.

How LERC will be defined based upon the ability to communicate and interactive communication capabilities between Low Impact Facilities that have BES Cyber Assets associated with them has yet to be fully vetted. The ability to communicate with a BES Cyber Asset isn't the same as interacting with the BES Cyber Asset. This distinction needs to be clearly defined. Another issue for Low Impact BES Cyber Systems is the need for a common definition of when serial devices are in scope and not in scope for consistent industry implementation.

Host-based security applications, advanced security threat analysis services, and cloud-based networks are not in scope for the SAR. There are mechanisms in place in the CIP standards that allow for exceptions, such as TFEs and CIP Exceptional Circumstances. ACES believes that these definitions could be expanded to include technology that exists outside of the standard to be able to be used, with approval, in order to provide the entity with a stronger defense in depth security profile.

If the drafting team proposes to modify definitions, they should consider a process that is non-prescriptive and provides flexibility for registered entities to decide how to best defend against cyber security threats based on their risk analysis. There may be significant advantages for industry to adopt new emerging security applications and cloud based security services. The CIP standards should not limit the tools or technology available to mitigate cyber security risks. We ask the drafting team to consider how the revisions to the CIP standards would allow for the power industry to match the security best practices of other industries against the latest security threats and vulnerabilities.

Thank you for your time and attention regarding this SAR.

Likes 0

Dislikes 0

Response

Erika Doot - 1,5

Answer

No

Document Name

Comment

The Bureau of Reclamation agrees with the drafting team's addition of "reviewing and addressing the CIP V5 requirements for CIP Exceptional Circumstances exceptions" to the SAR. However, Reclamation requests clarification on the scope of Guidelines and Technical Basis sections that may be changed with updates to the associated Standards within this project. Reclamation believes that addressing all CIP V5 Guidelines and Technical Basis sections within the scope of this revision may make the project unwieldy as it already contains a substantial scope of work to address FERC directives. Reclamation suggests that only Guidelines and Technical Basis sections related to standards language updates should be addressed within the scope of this project.

Likes 0

Dislikes 0

Response

Shannon Fair - 1,3,5,6, Group Name Colorado Springs Utilities

Answer

Yes

Document Name

Comment

CSU supports the standard drafting teams updates to the SAR.

Likes 0

Dislikes 0

Response

Thomas Foltz - 3,5

Answer

Yes

Document Name

Comment

AEP suggests that the SDT include separate balloting and commenting for Guidelines and Technical Basis throughout this project. With the development of implementation guidance, AEP is unsure whether the Guidelines and Technical Basis document should remain a part of the codified Reliability Standard. If it does, then stakeholders should have the ability to vote and comment on the contents specifically.

Likes 0

Dislikes 0

Response

Shannon Mickens - 2 - SPP RE, Group Name SPP Standards Review Group

Answer

Yes

Document Name

Comment

As our review group evaluated the revised SAR, we noticed that the V5TAG recommends providing clarity in the definitions of the two terms 'External Routable Connectivity (ERC)' and 'Interactive Remote Access (IRA). We suggest the drafting team either develop a new SAR or modify this one in order to require the term 'External Routable Connectivity (ERC)' to have the acronym and revised definition updated in the NERC Glossary and also included in the Rules of Procedure (RoP) for consistency and proper alignment. Additionally, we suggest the drafting team edit the SAR to review the Rules of Procedure where the acronym (IRA), is used to refer to 'Inherent Risk Assessment' whereas the CIP Standards refer to a term 'Interactive Remote Access' but do not use an acronym. There could be confusion if an acronym is used in either document for either of these terms. We suggest not using an acronym for either term in any document.

We also request clarification on why there is a specific deadline for updating the definition of LERC.

As for the term 'Low Impact External Routable Connectivity-LERC', we suggest the drafting team edit the SAR to clarify that a revised definition will also be included in the RoP.

When clarifying the 'lower bound' clarification in "adverse impact", we would appreciate a clear example (beyond the one used in the V5TAG document) that explains this concept.

We also request the SDT review or consider creating definitions or otherwise providing clarity for 'custom software' and the use of 'scripts'. There are several instances of regional inconsistencies in the scope of 'scripts' that should be included in an entity's baseline. Direction or clarity from this drafting team would be appreciated. Additional requirements or definitions may not be required, but guidance, rationale, or technical background would be beneficial.

Likes 0

Dislikes 0

Response

Stephanie Little - 1,3,5,6

Answer

Yes

Document Name

Comment

Arizona Public Service (AZPS) appreciates the opportunity to comment on the revised SAR, and submits the following comments previously provided in response to the initial SAR. Although AZPS generally supports the scope as described in the SAR, we believe that there are additional clarifications that should be considered beyond those detailed in the FERC Order 822 and the CIP Version 5 Transition Advisory Group (V5TAG) considerations.

AZPS believes the industry would benefit from clarification of the definition of the following terms:

- Transmission Facility – Transmission Facility is not a defined term. Although Facility is a defined term, AZPS does not believe that the Facility definition aligns with the standard's intent. AZPS suggests that a definition be provided by the Standard Drafting Team (SDT).
- Programmable - The SDT should consider defining programmable to clarify that a device would not be included simply because it was configurable, e.g., has functionality that can be changed locally.

AZPS would also like to suggest that the SDT clarify the intent of the grouping BCAs into BCS by leveraging the logically based perimeter security controls at the Electronic Security Perimeter (ESP) as well as local, device specific security controls per each BES Cyber Asset's (BCA) capability.

AZPS would also like to add some additional comments to the discussion in the V5TAG CIP V5 Issues for Standard Drafting Team Consideration document.

- AZPS recommends that the SDT consider not defining "adverse impact" or defining a lower bound thereof within the definition of BES Cyber Asset, but to revise the body of CIP standards and/or applicable defined terms to utilize already defined terms such as "Adverse Reliability Impact." Such would facilitate consistency as well as clarity regarding the N-1 contingency issue and other issues regarding that term identified by the V5TAG.
- AZPS believes that when BES Cyber Assets (BCA), such as relays, RTUs, and others, are connected via serial links to IP converters and/or IP-enabled security gateways, it would be appropriate to consider those elements downstream of the security gateways as BCA that do not have External Routable Connectivity (ERC). This is appropriate because the IP- converters and/or IP-enable security gateways require authentication and provide a protocol break. AZPS believes accurate and timely guidance related to serially connected devices supports the overall goal of providing appropriate and effective cyber security controls; thus, improving reliability.

- AZPS supports the CIP V5TAG analysis regarding virtualization. Virtualization is an effective tool for utilities and consideration should be given to ensuring that flexibility is maintained. An approach should consider the required outcome rather than the specifics of how that outcome is achieved.

AZPS also notes that NERC's webpage for this SAR "Project 2016-02 Modifications to CIP Standards", as of 4/11/2016, states the following:

"Also the scope of this work will incorporate existing and future RFIs relating to the CIP-002 through CIP-011 family of standards."

AZPS does not believe any RFIs are addressed in the current SAR. We recommend updating the SAR to reference existing submitted RFIs as appropriate. Finally, AZPS recommends removal from the SAR of functional registrations that are no longer included in the Compliance Registry, e.g., Interchange Authority, Load-Serving Entity and Purchasing-Selling Entity.

Likes 0

Dislikes 0

Response

Ruida Shu - 1,2,3,4,5,6,7 - NPCC, Group Name RSC

Answer Yes

Document Name

Comment

We support the revisions to the SAR.

Likes 0

Dislikes 0

Response

Andrea Jessup - 1,3,5,6 - WECC

Answer Yes

Document Name

Comment

BPA agrees with the revised scope of the SAR with three exceptions regarding the "Transmission Owner (TO) Control Centers Performing Transmission Operator (TOP) Obligations –" bullet and sub-bullets:

1. BPA proposes that the SDT clearly identify which function holds the compliance documentation responsibilities.
2. BPA believes the NERC Glossary definition of control center is adequate and should not be revised. The current definition maintains the distinction between control centers and substations.
3. BPA believes no clarification of the 'performs the functions of' language is needed for Attachment 1.

Likes 0

Dislikes 0

Response

larry brusseau - 1

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Colby Bellville - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Laura Nelson - 1

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Darin Ferguson - 1,3,5,7 - SERC

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - 10	
Answer	
Document Name	
Comment	
<p>Texas RE supports those comments suggesting that this project should identify continued areas for improvement within the existing CIP V5 Standards and avoid engaging in a wholesale “rewrite” of the CIP Standards at this point in time. Consistent with this principle, the Standards Drafting Team (SDT) has properly identified the FERC directives from Order No. 822 and the various V5 Tag recommendations as the framework upon which to base the scope of this project.</p> <p>However, Texas RE believes that the SDT should also take the opportunity to address two other areas to develop a strong record and enhance regulatory certainty around the application of the new suite of CIP Standards becoming effective on July 1, 2016. First, Texas RE agrees with those comments suggesting that the Commission should consider the interaction among the various CIP Standards, including the interaction between CIP-002-5.1 and the rest of the Standards as a group. The SDT may specifically wish to address the interplay between the various bright-line impact categories in the CIP-002-5.1 Standard and the risk assessments associated with the other CIP-005 Standards.</p> <p>Second, Texas RE recommends that the SDT explicitly consider and determine whether aspects of the various supporting materials associated with the CIP Standards, including a number of Lessons Learned, FAQs, and other guidance documents should be incorporated directly into the CIP Standards themselves. For example, the October 2015 CIP V5 Consolidated FAQs and Answers provided that “HVAV, UPS, and other support systems . . . will not be the focus of compliance monitoring” unless such systems are within an Electronic Security Perimeter. (p. 7). However, some HVAC and other systems may fall within the definition of a BES Cyber System and be subject, among other things, to the categorization requirements set forth in CIP-002-5.1, R1. The SDT could add clarity to the Standards by explicitly considering whether HVAC and other support systems should be (or is already) included within the BES Cyber System definition or conversely carved out of the CIP Standards in certain circumstances. This will encourage reliability and regulatory certainty by permitting entities to look to the Standard language to understand their compliance obligations, as well as produce a transparent record of the rationale underpinning a particular approach.</p> <p>Changes to SAR Redlined Language</p> <p>In addition to Texas RE’s suggestions regarding the scope of this project, Texas RE also suggests two additional revisions to the revised SAR language. First, the scope of the CIP Exceptional Circumstances exception language appears vague. Texas RE presumes that the SDT incorporated the recommendations from the Edison Electric Institute and others suggesting primarily that the SDT should consider whether the CIP Exceptional Circumstances exception should be added to additional CIP V5 requirements. Texas RE recommends making this more explicit by revising the SAR</p>	

language to state: "In addition, the SDT will review and address whether it is appropriate to include CIP Exceptional Circumstances exceptions within additional CIP V5 requirements."

Second, Texas RE supports the SDT's inclusion of language in the SAR permitting the SDT to make non-substantive changes to the Standards and Guidelines and Technical Basis sections to correct grammar, punctuation, and/or formatting errors. However, it is possible to read the proposed language to suggest that "errata" changes are somehow broader than such non-substantive revisions. Texas RE would suggest clarifying that "errata" changes to the CIP V5 Standards by inserting the word "non-substantive" in front of the word "errata" in the existing redline language.

Likes 0

Dislikes 0

Response