Comments
Received Report

Project Name:	2016-02 Modifications to CIP Standards SAR
Comment Period Start Date:	3/23/2016
Comment Period End Date:	4/21/2016
Associated Ballots:	

There were 33 sets of responses, including comments from approximately 33 different people from approximately 32 companies representing 9 of the Industry Segments as shown in the table on the following pages.

Questions

1. Do you agree with the scope and objectives of this SAR? If not, please explain why you do not agree, and, if possible, provide specific language revisions that would make it acceptable to you.

2. Are you aware of any Canadian provincial or other regulatory requirements that may need to be considered during this project in order to develop a continent-wide approach to the standards? If yes, please identify the jurisdiction and specific regulatory requirements.

3. Are there any other concerns with this SAR that haven't been covered in the previous questions?

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
Florida Municipal Power Agency	Chris Gowder	3,4,5,6	FRCC	FMPA	Tim Beyrle	Florida Municipal Power Agency	4	FRCC
					Jim Howard	Florida Municipal Power Agency	5	FRCC
					Lynne Mila	Florida Municipal Power Agency	4	FRCC
					Javier Cisneros	Florida Municipal Power Agency	3	FRCC
					Randy Hahn	Florida Municipal Power Agency	3	FRCC
					Don Cuevas	Florida Municipal Power Agency	1	FRCC
					Stan Rzad	Florida Municipal Power Agency	4	FRCC
					Matt Culverhouse	Florida Municipal Power Agency	3	FRCC
					Tom Reedy	Florida Municipal Power Agency	6	FRCC
					Steve Lancaster	Florida Municipal Power Agency	3	FRCC
					Mike Blough	Florida Municipal Power Agency	5	FRCC
					Mark Brown	Florida Municipal Power Agency	4	FRCC

					Chris Adkins	Florida Municipal Power Agency	3	FRCC
					Ginny Beigel	Florida Municipal Power Agency	9	FRCC
Duke Energy	Colby Bellville	1,3,5,6	FRCC,RF,SERC	Duke Energy	Doug Hils	Duke Energy	1	RF
					Lee Schuster	Duke Energy	3	FRCC
					Dale Goodwine	Duke Energy	5	SERC
					Greg Cecil	Duke Energy	6	RF
Southwest Power Pool, Inc. (RTO)	Jason Smith	2	MRO,SERC,SPP RE,WECC	SPP Standards Review Group	Shannon Mickens	Southwest Power Pool, Inc. (RTO)	2	SPP RE
					Jason Smith	Southwest Power Pool, Inc. (RTO)	2	SPP RE
					Ellen Watkins	Southwest Power Pool, Inc. (RTO)	1	SPP RE
					Terri Pyle	Southwest Power Pool, Inc. (RTO)	1,3,5,6	SPP RE
					Mike Buyce	Southwest Power Pool, Inc. (RTO)	1,4	SPP RE
Southern Company - Southern Company Services, Inc.	Pamela Hunter	1,3,5,6	SERC	Southern Company	Robert A. Schaffeld	Southern Company - Southern Company Services, Inc.	1	SERC
					R. Scott Moore	Southern Company - Southern Company Services, Inc.	3	SERC
					William D. Shultz	Southern Company - Southern Company Services, Inc.	5	SERC

					John J. Ciza	Southern Company - Southern Company Services, Inc.	6	SERC
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6	NPCC	RSC No Dominion	Paul Malozewski	Northeast Power Coordinating Council	1	NPCC
					Guy Zito	Northeast Power Coordinating Council	NA - Not Applicable	NPCC
					Brian Shanahan	Northeast Power Coordinating Council	1	NPCC
					Rob Vance	Northeast Power Coordinating Council	1	NPCC
					Mark J. Kenny	Northeast Power Coordinating Council	1	NPCC
					Gregory A. Campoli	Northeast Power Coordinating Council	2	NPCC
					Randy MacDonald	Northeast Power Coordinating Council	2	NPCC
					Wayne Sipperly	Northeast Power Coordinating Council	4	NPCC
					David Ramkalawan	Northeast Power Coordinating Council	4	NPCC

Glen Smith	Northeast Power Coordinating Council	4	NPCC
Brian O'Boyle	Northeast Power Coordinating Council	5	NPCC
Brian Robinson	Northeast Power Coordinating Council	5	NPCC
Bruce Metruck	Northeast Power Coordinating Council	6	NPCC
Alan Adamson	Northeast Power Coordinating Council	7	NPCC
Michael Jones	Northeast Power Coordinating Council	3	NPCC
Michael Forte	Northeast Power Coordinating Council	1	NPCC
Kelly Silver	Northeast Power Coordinating Council	3	NPCC
Brian O'Boyle	Northeast Power Coordinating Council	5	NPCC
Edward Bedder	Northeast Power Coordinating Council	1	NPCC
David Burke	Northeast Power	3	NPCC

						Coordinating Council		
					Peter Yost	Northeast Power Coordinating Council	4	NPCC
					Helen Lainis	Northeast Power Coordinating Council	2	NPCC
					Michele Tondalo	Northeast Power Coordinating Council	1	NPCC
					Kathleen Goodman	Northeast Power Coordinating Council	2	NPCC
					Silvia Parada Mitchell	Northeast Power Coordinating Council	4	NPCC
					Sylvain Clermont	Northeast Power Coordinating Council	1	NPCC
					Si Truc Phan	Northeast Power Coordinating Council	2	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

1. Do you agree with the scope and objectives of this 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 - Southwest Power Pool Regional Entity - 10	
Answer	No
Document Name	
Comment	

The SPP RE respectfully submits the following eight comments to the Project 2016-02 Standards Authorization Request: (1) With respect to clarifying or revising the definition of Cyber Asset, consider including misuse of the Programmable Electronic Device through misconfiguration or reconfiguration of the device in the instance that its behavior is affected and its altered behavior impacts the associated Facility. Consider the risk of misuse (i.e., how would someone misconfigure or reconfigure the device to cause undesired behavior) as appropriate. (2) With respect to clarifying or revising the definition of External Routable Connectivity (ERC), consider the point in the communication path at which a conversion from routable to non-routable communication protocol occurs. Is ERC only established if the conversion occurs in the same asset as the BES Cyber Asset or can ERC be established if the conversion occurs at the remote end of the communication path (e.g., conversion at the Control Center for communication to a serially connected relay in a substation)? Consider whether ERC exists only if the conversion occurs outside of an established ESP (i.e., there is no ERC if the device performing the conversion is inside an ESP and protected per the CIP Standards). (3) With respect to CIP-002-5.1, Impact Rating Criteria 3.2 and 3.3, clarify that the Low Impact BES Cyber Systems are associated with Facilities located within the asset as opposed to being associated with the asset itself. The opening statement in Section 3 of the Impact Rating Criteria states "BES Cyber Systems not included in Sections 1 or 2 above that are associated with any of the following assets…" The SPP RE has already been presented with an argument that flow meters in a substation are not BES Cyber Assets because they are associated with a Transmission line and not the Transmission station or substation cited in Impact Rating Criterion 3.2. (4) With respect to Tie Line and other Transmission line flow meters, these Cyber Assets appear to have been unintentionally excluded from consideration under CIP-002-5.1, Impact Rating Criterion 2.5. 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. (5) With respect to Physical Security Perimeters and their associated Requirements, clarification is needed regarding the concept of zoned access within a defined PSP. Specifically, is it acceptable to define an overarching PSP and then establish areas of access control within the defined PSP where BES Cyber Systems are present and for which different access permissions are established? For example, can a building containing a Control Center and its associated data center be declared a single PSP while access controls are established that do not permit all personnel with authorized unescorted access into the building to have authorized unescorted access into one or more access control zones within the building (e.g., the data center). And, if the zoned access areas are deemed to be independent PSPs, would the application of CIP-006-6 R1 Part 1.3 require two access controls to enter the interior PSP containing High Impact BES Cyber Systems, or would the requirement for two access controls to enter the outer (building) PSP suffice such that a single access control is permitted for the interior PSPs? (6) In consideration of the results of the investigation of the Ukraine cyberattack, the SPP RE recommends that Cyber Assets outside of the ESP with a machine-to-machine connection to a Cyber Asset inside the ESP be subjected to the same controls as the Intermediate System. There is a gap in the Standards today whereby a communication protocol typically used for interactive access (e.g., FTP, SSH, web services) can also be used for system-to-system communication. While Interactive Remote Access requires the use of an Intermediate System, encryption, and multi-factor authentication to the

Intermediate System, system-to-system communication using the exact same protocols do not require such controls. The Electronic Access Point cannot tell the difference, thus a successful compromise of the Cyber Asset residing outside of the ESP affords the attacker trusted access into the ESP. (7) In consideration of the results of the investigation of the Ukraine cyberattack, the SPP RE recommends the Standards Drafting Team consider whether essential support systems (UPS, PBX/VOIP phone, fire suppression, emergency generation) should be afforded certain protective controls to mitigate the risk that a successful attack directed at the support systems would adversely impact the asset containing BES Cyber Systems. For example, one element of the Ukraine attack was directed at a network-connected Uninterruptible Power Supply, removing power from essential Cyber Assets. (8) The SPP RE understands that a number of Requests for Interpretation have been submitted against CIP Version 5. While NERC staff has stated publicly that the RFIs would be addressed by the Standards Drafting team, there is no mention of RFIs in the Standards Authorization Request. To the extent that there are RFIs not included in either the Order 822 or V5TAG items, the Standards Authorization Request should state that pending RFIs will be considered and addressed in any revisions to the CIP standards.

Likes 0	
Dislikes 0	

Response

Steven Parker - EnergySec - NA - Not Applicable - NA - Not Applicable

Answer	No
Document Name	

Comment

We recommend that the term, Adverse Impact, contained within the BES Cyber Asset definition be itself added as a defined Glossary term. Any attempt to clarify this phrase by adding language within the BES Cyber Asset definition is likely to complicate, rather than simplify, understanding of the term.

The current outstanding Requests For Interpretation should be added as issues to be addressed by the Standards Drafting Team under this SAR. Per the Standards Process Manual, Section 7, Interpretations “shall stand until such time as the Interpretation can be incorporated into a future revision of the Reliability Standard.” Although this statement does not directly apply to the currently open, and unresolved, Requests for Interpretation, we believe the most logical approach would be to address the identified issues via this SAR rather than a separate interpretation development effort.

We recommend that the scope of the SAR be expanded to address the increasing use of 3rd party (i.e. cloud) services. Numerous utilities are leveraging new capabilities available from 3rd party providers in ways that enhance the overall security of the grid. Examples include cloud-based vulnerability scanners, offsite log monitoring services, cloud-based malware analysis and threat detection, cloud-based network monitoring, and colocation facilities. Unfortunately, the current standards are unduly prohibitive towards these services and as a result may be lowering the overall security of the grid by discouraging the use of effective, cutting edge tools, techniques, and services. For example, CIP-006 requires EACMS devices to be within a Physical Security Perimeter. It is not clear how, or if, this requirement can be met for cloud services. The SDT should review existing language and add, modify, or remove language as needed to accommodate any such services that can be prudently deployed to enhance overall grid security.

Likes 0	
Dislikes 0	

Response

Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE	
Answer	No
Document Name	

Comment
Xcel Energy has some concern that the SAR's inclusion of communication network components between control centers could extend to cabling between Control Centers. The inclusion of cabling between Control Centers would be in direct contrast to guidance in the CIP standards and the authority granted in section 215(d)(5) of the FPA by asking entities to be held accountable for equipment they do not own. Communication networks between discrete Electronic Security Perimeters (ESPs) have been excluded from the CIP standards. Additionally, it is unclear how physical protection of cabling would afford any additional protection to networks already in compliance with the suite of CIP standards. Furthermore, the documentation of any physical protection would be administratively burdensome without adding any additional protection. If any requirement is to be added regarding cabling between Control Centers, we would encourage the drafting team to add it as logical controls such as encryption or other such measures under CIP-005 and/or CIP-007. To require physical protection of equipment not owned by Registered Entities seems in direct contrast to previous guidance, outside of the authority documented in section 215(d)(5) of the FPA and add administrate burden with little value.

Likes 0	
Dislikes 0	

Response

Ginny Beigel - City of Vero Beach - 9	
Answer	No
Document Name	

Comment
See response to Question 3.

Likes 0	
Dislikes 0	

Response

Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	No
Document Name	
Comment	
SMUD respectfully suggests an addition to the objective for this SAR be modified to include addressing single points of failure in communication networks and network equipment that meet the definition of the BCA where this equipment is outside of the ESP but contained within the Facility.	
Likes 0	
Dislikes 0	
Response	

Maryclaire Yatsko - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	No
Document Name	
Comment	

Seminole concurs with all items currently listed in the draft Standards Authorization Request. Seminole recommends that additional items should be included in the SAR

The industry has received guidance from NERC's Compliance Monitoring and Enforcement group in the form of Frequently Asked Questions and Lessons Learned. These guidance items need to become formal Guidelines, with appropriate Technical Basis, and placed within the Standards and approved by the NERC membership

Issues related to Shared Facilities that are not adequately addressed in the standards. Specifically, when multiple entities have BES Cyber Assets residing at a shared location, there is no clear delineation of responsibility. Without defined responsibilities in the Standard, there is also no documented process to determine who has responsibility and to document those responsibilities. CFRs, JROs, MOUs, and other contractual agreements have been discussed as possible solutions to this issue. However, at a minimum, clear formal Guidelines should be added to CIP-002-5.1. Additional guidance should be added where appropriate.

Based on experience of both the V5TAG and of entities preparing for the standards, it is clear that significant updates are needed to the Guidelines and Technical Basis for all CIP Reliability Standards.

Based on these comments, Seminole recommends adding language to address the following items:

1. **Guidelines and Technical Basis** – As core information used by Entities to ensure a consistent understanding of requirements and based on Lessons Learned by Entities, Reliability Standards CIP-002 through CIP-011 are authorized for modification by the Standards Development Team and submitted for ballot to the NERC Ballot Body. These clarifications should minimally consider
    i. Lessons Learned and FAQs published by NERC and Regional Compliance
    ii. Items that may be determined unsupported by the standard and definitions (i.e. BES Reliability Operating Services); and
    iii. Industry practices that have evolved from industry's compliance efforts.
2. **Paragraph 51 option** - Option to consider removal of Requirement Parts in specific cases considering the same guidelines as those used in the Paragraph 51 project.
3. **Definitions of Low Impact External Routable Connectivity AND External Routable Connectivity** - Consider modifying the definitions of External Routable Connectivity and LERC to ensure consistent language and communication of both ERC and LERC definitions
4. **Definitions of Cyber Asset, BES Cyber Asset (BCA), and BES Cyber System (BCS)** – The SAR should also authorize changes to clarify the definition of BES Cyber System, specifically whether BES Cyber Systems include any Cyber Asset type other than a BCA (such as PCA, EACMS, PACS)
5. **Measures and Audit Expectations** - Using information provided by the NERC Compliance Monitoring group as one source of information, the measures section of all requirements and requirements parts should be reviewed and updated as necessary to ensure that an entity who provides the evidence listed in the measure is able to fully demonstrate compliance under normal circumstances.
6. **Exceptional Circumstances** - Recommend formalizing guidance for Exceptional Circumstances in a single location.

Likes 0	
Dislikes 0	

Response

Andrew Pusztai - American Transmission Company, LLC - 1

Answer	No
Document Name	

Comment

ATC is a member of EEI and supports the comments submitted by the EEI CIP Standards Subgroup related to the draft SAR.

Likes 0	

Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE	
Answer	No
Document Name	
Comment	
The Edison Electric Institute (EEI) submitted comments relating to this SAR. Their comments address scope and objectives of the SAR for consideration by the Standards Drafting Team. Kansas City Power & Light Company endorses and incorporates by reference the comments submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6 - NPCC, Group Name RSC No Dominion	
Answer	No
Document Name	
Comment	
Request that the scope of virtualization be expanded beyond only CIP-005. Want to remind the SDT that communications between Control Centers usually involves third parties that tend to be outside of FERC’s jurisdiction.	
Likes 0	
Dislikes 0	
Response	
Ryan Walter - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	No
Document Name	

Comment
The phrase “control centers” in the “Industry Need” section which lists the FERC directives has not been capitalized. FERC Order 822 uses “bulk electric system Control Centers” when speaking about this directive. Tri-State believes the SAR should use that same language used by FERC in order to accurately represent what is expected to be in scope of this project. There is also an error in the “Reliability Functions” section. “Transmission Service Provider” is checked off instead of “Distribution Provider”. The new versions of the CIP standards do not include Transmission Service Providers, but do include the Distribution Providers.

Likes 0	
Dislikes 0	

Response

Mike Smith - Manitoba Hydro - 1,3,5,6	
Answer	No
Document Name	

Comment
Virtualization: Manitoba Hydro does not agree with NERC prescribing specific system architecture, technologies or designs. The SDT should continue to focus on identifying requirements to meet specific security objectives for the virtualization. Protections for communication network components between control centers: Please clarify the scope of Control Centers. Does it refer to the communication links between all Control Centres cross entities such as the link between RC Control Center and TOP Control Centre or only the Control Centers within the resposbile entity.

Likes 0	
Dislikes 0	

Response

Chris Gowder - Florida Municipal Power Agency - 3,4,5,6 - FRCC, Group Name FMPA	
Answer	No
Document Name	

Comment

FMPA is concerned that the Project 2016-02 SAR is too narrowly focused. There are a number of issues with the current CIP Standards, mostly concentrated in CIP-002-5.1. The SAR should be written to allow the drafting team to consider how the suite of CIP standards work together. CIP-002-5.1 is the foundation of the remainder of the CIP requirements. Narrowly scoping this SAR just prolongs dealing with these problems, and ties the drafting team's hands should they identify other concerns. Also, ignoring these issues now will cause more revisions, which in turn will add to the pervasive confusion and uncertainty already surrounding the CIP standards. The industry needs clarity and resolution to these matters in order to be assured their efforts to comply are effective and that companies understand their investments are going to the right places.

The following additional items should be considered by the SDT:

1) Section 4.2.2 states "All BES Facilities" as being subject to the standards for all Responsible Entities except for DP's. This effectively negates the rest of the requirements, as anything that qualifies as a "Cyber Asset" could not possibly be a "Facility" as well. The language is missing the "Cyber Assets" component. Suggested language would be "Cyber Assets at all BES Facilities".

2) Ownership isn't properly accounted for in the requirements. Shared facilities (generally speaking substations) often involve multiple entities that own equipment, who may or may not be Responsible Entities as described in CIP-002-5.1. There should be specific language requiring the owner of the equipment to communicate with the owner of the Facility.

3) Clarify what is meant by "associated with" in the context of the Impact Rating Criteria in CIP-002-5.1 – Attachment 1. Clear up the inconsistencies in the requirements between the use of "associated with" (criterion 2 & 3 in Attachment 1) in some areas and "used by and located at" (criterion 1 in Attachment 1) in other parts. Have a process developed for ensuring entities notify if there are devices owned by a different entity that are "associated with" their BESCS (for example, a meter that one entity needs for the reliable operation of their Control Center that isn't owned by them).

4) Leasing equipment is a loophole in the requirements based on the language in section 4.2. This should be fixed so an entity isn't able to lease equipment and avoid meeting CIP requirements.

5) The scope of equipment applicable to CIP due to applicability to other NERC standards (such as CIP-002-5.1 Section 4.2.1.3) should be clarified further. For example, a "Protection System" can be made up of multiple devices owned by multiple entities. If an entity owns a component of a Protection System that isn't a Cyber Asset, they shouldn't have to meet CIP requirements.

6) Voice over Internet Protocol (VoIP), much like virtualized servers and environments, is not discussed in the CIP requirements. VoIP telephony devices should be excluded from the requirements unless they are networked with other BESCS, in which case they could become protected CA's.

7) There is no mention of "data at rest" in this SAR, although it was clearly part of Order 822 (paragraph 56 – "NERC's response to the directives in this Final Rule should identify the scope of sensitive bulk electric system data that must be protected and specify how the confidentiality, integrity, and availability of each type of bulk electric system data should be protected while it is being transmitted **or at rest**").

8) CIP-002-5.1 should be re-written to make sure all assets are properly identified. For example, under R1 of CIP-002-5.1, a Responsible Entity is only required to find Cyber Assets at each of the six locations listed under R1. However, in Attachment 1 for medium and low impact, the language of "associated with" is introduced, indicating that there could be assets/locations containing Cyber Assets that are not part of the list of six asset types listed under R1. The approach taken by R1 is not the one being recommended by NERC or the Regional Entities. The standard should be revised to clarify the relationship between the six asset types/locations in R1 and the "used by and located at"/ "associated with" language in Attachment 1.

Likes 0	
Dislikes 0	
Response	

Matt Stryker - Georgia Transmission Corporation - 1 - SERC	
Answer	No
Document Name	
Comment	

The SAR should be modified to include the following language and scope:Update obsolete references to NERC defined terms or standards through modifications to the CIP standards. References which are obsolete or require clarification include, but are not limited to:

- To improve consistency within Registered Entity compliance programs, phrasing in CIP-002-5.1 Requirement 1 and Attachment 1 referencing undefined or unclear terms or phrases such as “Transmission stations and substations”, “generation interconnection Facilities”, “Systems and facilities critical to system restoration”, “Generation resources”, “BES reactive resource or group of resources” should be removed by the SDT and instead reference the FERC approved definition of Bulk Electric System (BES) which now included clear and defined qualifications for inclusion and exclusion of these assets as well as an appeals process to address exceptions. An example would be changing the following language:
- R1.ii. Stations and Substations containing BES Facilities
- R1.iii BES Generation Facilities
- RAS: Phrasing in CIP-002-5.1 Applicability, Requirement 1, and Attachment 1 referencing variations of Special Protection System (SPS), Remedial Action Scheme (RAS), or automated switching System that operates BES Elements should be clarified and simplified by the SDT to reference the new Remedial Action Scheme (RAS) definition which FERC approved 11/19/2015.
- The current PSP definition should be clarified by the SDT to address that it should not apply to assets in CIP-006-6 Part 1.1 simply because they may be secured in a location which meets the PSP definition: “The physical border surrounding locations in which BES Cyber Assets, BES Cyber Systems, or Electronic Access Control or Monitoring Systems reside, and for which access is controlled.”
- Interactive Remote Access definition: The SDT should clarify the phrase “system-to-system process communications” to address scripts or batch operations performed on-demand or on a periodic basis as not meeting the definition.
- The phrase “Collector Bus” as it appears in Attachment 1, Criteria 2.4 and 2.5 should be defined by the SDT. The guidance document references a report (*Final Report from the Ad Hoc Group for Generation Requirements at the Transmission Interface*) which predated the adoption of the NERC BES definition and has not been picked up for development since. The BES definition provides additional clarification of the applicability to multiple generation scenarios in I2, I4, E1, E2, E3, and E4. Notably, CIP-014-1 does provide a diagram of the collector bus, but does not include an associated definition.
- Attachment 1, Criterion 2.4: Clarify if the Transmission Facilities operated at 500kV or higher are “at a single station or substation” to make the language and application consistent with Criterion 2.5 to correctly scope BES Cyber Assets.
- Clarify CIP-002-5.1 R1.vi for Registered Entities registered for additional functions other than Distribution Providers. Revising the language of CIP-002-5.1 R1.vi. to state “*For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above at assets which have not already been considered under Ri-Rv*” would be a possible solution.

Likes 0	
Dislikes 0	

Response

Shannon Fair - Colorado Springs Utilities - 1,3,5,6, Group Name Colorado Springs Utilities	
Answer	Yes
Document Name	
Comment	
Colorado Springs Utilities agrees with the scope of the SAR.	
Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	Yes
Document Name	
Comment	
No comment	
Likes 0	
Dislikes 0	
Response	
Erika Doot - U.S. Bureau of Reclamation - 1,5	
Answer	Yes
Document Name	
Comment	
The Bureau of Reclamation believes that the proposed Standards Authorization Request addresses FERC directives in Order No. 822. Reclamation also supports NERC efforts to address the issues identified by the CIP Version 5 Transition Advisory group.	
Likes 0	
Dislikes 0	

Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	

Idaho Power agrees with the items that are currently scoped into the SAR, but also believe it does not go far enough. There are numerous areas within the v5/v6 standards where clarifications need to be made. Idaho Power doesn't think that a full re-write of all of the CIP standards is prudent as it will create continued churn in the industry. Idaho Power believes there should be continual slow improvement in the standards and not large swings that create guidance gaps from the regulators and understanding gaps from the industry.

The proposed scope does not include a change to the applicability columns to tier ratings (i.e., medium with and without ERC). These need to be more explicitly split out as they create odd breakdowns in the standards that seem to be creating inconsistencies in the standards. For example, under CIP-010-2 R4 Attachment 1, R1.2 requires authorizations for all Transient Devices and R3.1 for removable media for Medium Impact BCS. However, Medium Impact BCS without external routable connectivity (ERC) do not require an authorization records under CIP-004, specifically R4.1. This means the critical devices/systems themselves have no authorization requirements, but the transient devices and removable media associated with them do. A second example is information protection for Medium Impact BCS without ERC. CIP-011-2 requires information protection policies/procedures be applied equally to all Medium Impact BCS, which includes protecting it in storage, transit, and use. However, once again, there are no requirements to authorize an individual to gain access to "designated storage locations" under CIP-004-6 Part 4.1.3. This means the information needs to be protected, but only those Medium BCS with ERC have to have individuals get authorized for access to the information. This seems consistent with not authorizing individuals to get access to Medium Impact BCS without ERC but not with applying information protection policies to one tier of Medium Impact BCS.

The SDT should consider four risk tiers rather than three if they are going to treat ERC and non-ERC separately in the standards. These are simply two examples of inconsistencies that have been created by trying to treat them within the same "medium" risk tier. There could still be similar requirements that would be applied to a Medium Impact BCS with ERC and a Medium Impact BCS without ERC, but inconsistencies would be more easily identified by breaking out the Medium BCS tier and the Medium without ERC.

The proposed scope does not include changes to CIP-002-5.1. CIP-002 has several inconsistencies and logic issues and no clearly delineated process allowing no clear way to comply with the standard other than simply deciding on a direction and hoping the regional entity is okay with your approach. The wording and processes required by CIP-002 need to be refined and clarified to make the expectations more clearly known. For example, the Guidelines and Technical Basis state, "The following provides guidance that a Responsible Entity may use to identify the BES Cyber Systems that would be in scope. The concept of BES reliability operating service is useful in providing Responsible Entities with the option of a defined process for scoping those BES Cyber Systems that would be subject to CIP [illegible] reference to use of the BROS is stated as an option that may be useful in identifying BCAs/BCSs. Nowhere in CIP-002 the definition of BCA or BCS does it speak directly to the BROS. The only loose tie-in is that the definition of BCS talks about reliability tasks, which FERC, in Order 791, clarified they believed it alluded to the NERC Functional Model, which relates to the high-level responsibilities of registered entities. However, it seems regions are beginning to take a stance that BROS is the hard-line approach as the only acceptable way to approach identification of CIP assets and BCAs/BCSs. Additionally, the wording of the CIP-002 standard does not ever specifically state that an entity needs to identify Protected Cyber Assets (PCAs), Electronic Access Control or Monitoring System (EACMS) or Physical Access Control Systems (PACS), yet the standards expect that entities will know what those devices are in order to apply specific requirements to them. Entities should not have to read between the lines when trying to comply with mandated compliance standards. Doing so creates confusion, inconsistencies, and distrust between the regulators and the industry who should be working together to meet common objectives.

Likes 0	
Dislikes 0	
Response	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
ERCOT recommends that *Project 2016-02 – Modification to CIP standards* be limited to 1.) clarifying existing language,2.) addressing the V5 TAG issue list, and 3.) incorporating the FERC-directed changes discussed in FERC Order No. 822. Introducing new concepts through substantive language changes in this iteration would be premature. In order to allow CIP Version 5 and 6 concepts to be fully implemented, any proposed substantive changes should be reserved for future CIP standards projects.	
Likes 0	
Dislikes 0	
Response	
Andrew Gallo - Austin Energy - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	
Although Austin Energy (AE) agrees with the SAR's objectives, we urge the SDT to proceed with caution. Registered Entities are just now reaching compliance with the Version 5/6 Standards. Unless a device truly creates risk to the BES, we should not include it in the CIP Standards' scope.	
Likes 0	
Dislikes 0	
Response	
Jeri Freimuth - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes

Document Name	
Comment	

Arizona Public Service (AZPS) appreciates the opportunity to comment on the proposed 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.

Likes 0	
Dislikes 0	
Response	
Warren Cross - ACES Power Marketing - 1,3,5,6 - MRO,WECC,Texas RE,SERC,SPP RE,RF	

Answer	Yes
Document Name	
Comment	
Look to NIST 800-125 for virtualization security.	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Burns & McDonnell - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Diana McMahon - Salt River Project - 1,3,6,7 - WECC	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Sistrunk - Small End-Use Electricity Customer - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Langston - Tallahassee Electric (City of Tallahassee, FL) - 1,3,5	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Williams - Tallahassee Electric (City of Tallahassee, FL) - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jason Smith - Southwest Power Pool, Inc. (RTO) - 2 - MRO,SPP RE, Group Name SPP Standards Review Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

2. Are you aware of any Canadian provincial or other regulatory requirements that may need to be considered during this project in order to develop a continent-wide approach to the standards? If yes, please identify the jurisdiction and specific regulatory requirements.	
Richard Vine - California ISO - 2	
Answer	No
Document Name	
Comment	
No comment	
Likes 0	
Dislikes 0	
Response	
Matt Stryker - Georgia Transmission Corporation - 1 - SERC	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Gowder - Florida Municipal Power Agency - 3,4,5,6 - FRCC, Group Name FMPA	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Mike Smith - Manitoba Hydro - 1,3,5,6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ryan Walter - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Warren Cross - ACES Power Marketing - 1,3,5,6 - MRO,WECC,Texas RE,SERC,SPP RE,RF	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jason Smith - Southwest Power Pool, Inc. (RTO) - 2 - MRO,SPP RE, Group Name SPP Standards Review Group	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6 - NPCC, Group Name RSC No Dominion	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jeri Freimuth - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrew Gallo - Austin Energy - 1,3,4,5,6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	

Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Williams - Tallahassee Electric (City of Tallahassee, FL) - 1,3,5	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Langston - Tallahassee Electric (City of Tallahassee, FL) - 1,3,5	
Answer	No

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrew Pusztai - American Transmission Company, LLC - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Maryclaire Yatsko - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	No
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Chris Sistrunk - Small End-Use Electricity Customer - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	No
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Diana McMahon - Salt River Project - 1,3,6,7 - WECC	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ginny Beigel - City of Vero Beach - 9	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE	
Answer	No
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Steven Parker - EnergySec - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Erika Doot - U.S. Bureau of Reclamation - 1,5	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Michael Johnson - Burns & McDonnell - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bob Reynolds - Southwest Power Pool Regional Entity - 10	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Shannon Fair - Colorado Springs Utilities - 1,3,5,6, Group Name Colorado Springs Utilities	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response

3. Are there any other concerns with this SAR that haven't been covered in the previous questions?	
Warren Cross - ACES Power Marketing - 1,3,5,6 - MRO,WECC,Texas RE,SERC,SPP RE,RF	
Answer	No
Document Name	
Comment	
The SDT should prioritize the issues based on whether it is associated with a FERC directive or not. For issues that are not directed by FERC, there may need to be additional time to find a resolution associated with these issues. The only deadlines on this project are related to the FERC directives.	
Likes 0	
Dislikes 0	
Response	
Shannon Fair - Colorado Springs Utilities - 1,3,5,6, Group Name Colorado Springs Utilities	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bob Reynolds - Southwest Power Pool Regional Entity - 10	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Erika Doot - U.S. Bureau of Reclamation - 1,5	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Parker - EnergySec - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	2016-02_CIP_SAR_Unofficial_Comment_Form_ERCOT draft.docx
Comment	
Likes 0	
Dislikes 0	
Response	

Maryclaire Yatsko - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Langston - Tallahassee Electric (City of Tallahassee, FL) - 1,3,5	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Williams - Tallahassee Electric (City of Tallahassee, FL) - 1,3,5	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	

Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrew Gallo - Austin Energy - 1,3,4,5,6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jason Smith - Southwest Power Pool, Inc. (RTO) - 2 - MRO,SPP RE, Group Name SPP Standards Review Group	
Answer	No

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ryan Walter - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1,3,5,6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Matt Stryker - Georgia Transmission Corporation - 1 - SERC	
Answer	No
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Burns & McDonnell - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	

Burns & McDonnell appreciates the opportunity to comment on the Standard Authorization Request (SAR) titled “Modifications to CIP Standards” with the following input:

The V5TAG recommended the Standard Drafting Team (SDT) consider Virtualization as part of the SAR due to the increased use of this technology in industry control system environments. Burns & McDonnell is recommending the Virtualization section of the SAR be amended to indicate that the SDT not only consider virtualization technology usage by Responsibility Entities (Entity) which they own and operate, but usage of similar technology not owned or operated by an Entity. Increased interest in “cloud” based services such as Software as a Service (SaaS) and Platform as a Service (PaaS) have created questions on the application of the standards with no guidance on how they should be applied. Cloud usage of virtual technology is similar to Entity owned usage of the same technology, but Burns & McDonnell feels it is important that both usage conditions be considered and any differences in approach be indicated in any final SDT work product. Burns & McDonnell does not believe a separate section should be created for “cloud” usage, but the SAR section on Virtualization could be updated to cover virtualization technology owned by or usage of services by an Entity. One recommendation for the re-wording is:

The CIP V5 standards do not specifically address virtualization. Because of the increasing use of virtualization in industrial control system environments either owned and operated by a Responsible Entity, or from a service provider who owns and operates the environment under the service providers control, V5TAG asked that the SDT consider CIP-005 and the definitions of Cyber Asset and Electronic Access Point regarding permitted architecture and the security risks of network, server and storage virtualization technologies under these two type of conditions.

Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	Yes
Document Name	

Comment
Currently there are no specific requirements or guidelines included within the NERC CIP Reliability Standards v.5/6 relating to utilization of the cloud. Based on discussions with the regional auditing body, it has been agreed upon that utilization of the cloud for storage of BES Cyber System Information may be sufficiently secured through field level packet encryption with the responsible entity only holding the private key. It would be in the interest of the California ISO for there to be a provision included within the NERC CIP Reliability Standards addressing cloud scenarios.

Likes 0	
Dislikes 0	

Response

Ginny Beigel - City of Vero Beach - 9	
Answer	Yes
Document Name	

Comment
We belong to the FMPA municipal organization and have arrived at a consensus with the help of one of its SMEs who is immersed in CIP Standards. Comments follow below: The SAR falls short of fixing a lot of the core issues related to CIP-002-5.1. The following additional items should be addressed by the SDT: 1) Section 4.2.2 states “All BES Facilities” as being subject to the standards for all Responsible Entities except for DPs. This effectively negates the rest of the requirements, as anything that qualifies as a “Cyber Asset” could not possibly be a “Facility” as well. The language is missing the “Cyber Assets” component. Suggested language would be “Cyber Assets at all BES Facilities.” 2) Ownership isn’t properly accounted for in the requirements. Shared facilities (generally speaking substations) often involve multiple entities that own equipment, who may or may not be Responsible Entities as described in CIP-002-5.1. There should be specific language requiring the owner of the equipment to communicate with the owner of the Facility. 3) Clarify what is meant by “associated with” in the context of the Impact Rating Criteria in CIP-002-5.1 – Attachment 1. Clear up the inconsistencies in the requirements between the use of “associated with” (criterion 2 & 3 in Attachment 1) in some areas and “used by and located at” (criterion 1 in Attachment 1) in other parts. Have a process developed for ensuring entities notify if there are devices owned by a different entity that are “associated with” their BESCS (for example, a meter that one entity needs for the reliable operation of their Control Center that isn’t owned by them).

4) Leasing equipment is a loophole in the requirements based on the language in section 4.2. This should be fixed so an entity isn't able to lease equipment and avoid meeting CIP requirements.

5) The scope of equipment applicable to CIP due to applicability to other NERC standards (such as CIP-002-5.1 Section 4.2.1.3) should be clarified further. For example, a "Protection System" can be made up of multiple devices owned by multiple entities. If an entity owns a component of a Protection System that isn't a Cyber Asset, they shouldn't have to meet CIP requirements.

6) Voice over Internet Protocol (VoIP), much like virtualized servers and environments, is not discussed in the CIP requirements. VoIP telephony devices should be excluded from the requirements unless they are networked with other BESCS, in which case they could become protected CA's.

7) There is no mention of "data at rest" in this SAR, although it was clearly part of Order 822 (paragraph 56 – "NERC's response to the directives in this Final Rule should identify the scope of sensitive bulk electric system data that must be protected and specify how the confidentiality, integrity, and availability of each type of bulk electric system data should be protected while it is being transmitted **or at rest**").

8) CIP-002-5.1 should be re-written to make sure all assets are properly identified. For example, under R1 of CIP-002-5.1, a Responsible Entity is only required to find Cyber Assets at each of the six locations listed under R1. However, in Attachment 1 for medium and low impact, the language of "associated with" is introduced, indicating that there could be assets/locations containing Cyber Assets that are not part of the list of six asset types listed under R1. The approach taken by R1 is not the one being recommended by NERC or the Regional Entities. The standard should be revised to allow for the proper capture of all Cyber Assets either ONLY at the six asset locations, OR both at these locations as well as any other associated location.

Likes 0	
Dislikes 0	
Response	
Diana McMahon - Salt River Project - 1,3,6,7 - WECC	
Answer	Yes
Document Name	
Comment	

For network and externally accessible devices, SRP agrees with improving clarity within the concepts and requirements concerning Electronic Security Perimeters (ESP), External Routable Connectivity (ERC), and Interactive Remote Access (IRA). However, SRP has additional concerns.

Although much of CIP-005-5 is compatible to CIP V3 requirements, it does include a new requirement related to IRA for High Impact BES Cyber Systems and Medium Impact BES Cyber Systems with ERC. R2.1 states: *Utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.*

Based on R2.1 and the defined terms, demonstrating compliance with this requirement fundamentally requires evidence of two items:

1. That an Intermediate System is utilized such that the Cyber Asset initiating IRA does not **"directly access"** an applicable Cyber Asset; and

2. That technology for facilitating IRA meets the definition of an Intermediate System.

Issues with #1 – Ambiguity of "Directly Access"

In SRP's experience the ERO and Regional Entities have used undefined terminology such as "protocol break", "OSI layer 7 application break", "session break" and others to describe what is intended by or compliant with the phrase "does not directly access". However, SRP believes these terms mean different things to different subject matter experts and auditors. FERC articulated as much in Order 822. Although this issue has focused on LERC/LEAP requirements for low impact assets, the same ambiguity exists in the requirements for high/medium impact facilities. Where standards are unclear or ambiguous, entities are typically afforded flexibility in their compliance approaches. However, SRP believes the ERO has taken a rather prescriptive view of these requirements where reasonable people could easily differ in their interpretation. These ambiguities in defined terms and requirements need to be addressed by the SDT.

Issues with #2 – Ambiguity on acceptable Intermediate Systems

As noted in the Glossary of Terms, an Intermediate System is an Electronic Access Control or Monitoring System (EACMS). That notwithstanding, the ERO and Regional Entities have articulated rather informally and only fairly recently a need to assess each Intermediate System against the definition of BES Cyber Asset. This creates the potential for the proverbial "hall of mirrors" result, in the sense that individuals can rationalize a circumstance where seemingly all Cyber Assets (PACS, EACMS, other) could, under some scenario qualify as a BES Cyber Asset. SRP believes this was clearly not the intent of the Standard Drafting Team, and SRP does not believe this concept was considered for Intermediate Systems evaluated during the CIP V5 pilot project.

Most specifically, an entity that was on the drafting team and participated in the implementation pilot project with no issues was "surprised" with the Regional Entity's assessment of compliance on this subject at time of audit. There is clearly a disconnect that needs to be addressed.

Architectures to support Interactive Remote Access to high, medium impact control centers, transmission stations and generation resources are very costly. Current ambiguity could cause extensive and rework for high and medium impact systems, and be even more impactful if similar architectures are applied to low impact assets.

The Standards Drafting Team (SDT) must clearly define the term "direct access" for high and medium facilities, ensuring "direct access" has same meaning for low impact facilities as ordered by FERC in its approval of the CIP V5 revisions. To the extent different controls are appropriate for high/medium vs. low impact systems, those distinctions must be clear in the language of the standard. SRP further recommends the SDT re-evaluate the definitions of Interactive Remote Access, Intermediate System, and BES Cyber Asset to ensure entities have a clear understanding of the security and compliance expectations associated with the standards.

Likes 0	
Dislikes 0	
Response	
Chris Sistrunk - Small End-Use Electricity Customer - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	

I believe that the CIP standards do not properly address security monitoring of networks (routable and non-routable). In my experience in the security industry that breaches (like electric disturbances) are inevitable, even for control systems. It's a matter of when, not if. The Security Event Monitoring logging requirements in CIP 007-5 R4 is a start, but I don't believe this data (4.1.1. Detected successful login attempts; 4.1.2. Detected failed access attempts and failed login attempts; 4.1.3. Detected malicious code.) provides enough digital forensic evidence in the aftermath of an intrusion or even a cyber attack. Also, the retention period in 4.3 of a minimum of "90 consecutive calendar days" is not sufficient. According to the 2016 M-Trends Report from FireEye (https://www2.fireeye.com/rs/848-DID-242/images/Mtrends2016.pdf), the median time of network compromise to discovery of the attacker is 146 days. If a utility only kept 90 days of logs, then it's quite possible that they won't have the forensics data to determine if the attacker used stolen credentials or malicious code. Also, many utilities don't use authentication or encryption with their Control System Protocols such as DNP3, ICCP, and Modbus. If an attacker were to spoof, replay, or modify the SCADA traffic, this would not be detected by the current set of monitoring and logging requirements.

However, IT security best practice of network security montoring (NSM) does provide sufficient network forensics data. NSM is similar to the type of monitoring and visibility required by NERC PRC 002-2 Disturbance Monitoring and Reporting standard. I wrote a blog post (https://www.linkedin.com/pulse/comparing-nerc-disturbance-monitoring-reporting-network-sistrunk) about the similarities between PRC 002-2 and NSM...and how NERC CIP 007 R4 could be improved to provide a bit more forensics data. Collecting NSM type data such as Session Data (timestamp, source IP address, source port, destination IP, destination port at a minimum) does not require a lot of storage space and would provide a better level of visibility. Collecting a shorter time period of full network packet captures for High or Medium BES Cyber Systems (including non-routable dial-up access) also is not very complicated, as IT systems have been doing this a long time.

Since BES systems are becoming more connected, we cannot ignore network security monitoring in the future. I hope it doesn't take a serious cyber incident to convince the need for monitoring...much like the 1965 and 2003 blackouts convinced us to do disturbance monitoring. I know we haven't had a cyber attack that caused a power outage here in North America, but as an Electrical Engineer who has worked in the electric utility industry, now representing the ICS security industry, and also a customer, I want to help ensure that this doesn't happen.

Likes 0	
Dislikes 0	
Response	

Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Duke Energy requests that the SDT consider revisiting the transfer of employees and the requirement to remove access for that employee in 1 calendar day which may be viewed as overly burdensome. While this may be outside the scope of this particular SAR, we feel that since the project is regarding revisions to CIP standards, that we would be remiss not to request further discussion around this topic.	
Likes 0	
Dislikes 0	
Response	
Andrew Pusztai - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
ATC is a member of EEI and supports the comments submitted by the EEI CIP Standards Subgroup realted to the draft SAR. Please review for applicability to this question.	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Texas RE noticed there is a statement on page 4 which says the compliance deadline is April 1, 2016. This has been moved back to July 1, 2016.	

Likes 0	
Dislikes 0	
Response	
Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	

In addition to the issues addressed by the SAR, the Edison Electric Institute, on behalf of our members, recommends that the proposed project also consider the following ten issues:

Issue 1: CIP Exceptional Circumstances

A CIP Exceptional Circumstance is defined as:

"A situation that involves or threatens to involve one or more of the following, or similar, conditions that impact safety or BES reliability: a risk of injury or death; a natural disaster; civil unrest; an imminent or existing hardware, software, or equipment failure; a Cyber Security Incident requiring emergency assistance; a response by emergency services; the enactment of a mutual assistance agreement; or an impediment of large scale workforce availability."

We appreciate the understanding and recognition for the need to enable provisions for CIP Exceptional Circumstances. However, during implementation of CIP V5, it has become apparent that the CIP Exceptional Circumstances provision may need to be added to several requirements. Below are a few situation-based examples:

- *Risk of injury or death*: CIP-004-6 R2 and R4 allow for CIP Exceptional Circumstances to waive the need for Training and the Authorization based on need to be waived during such circumstances. We believe that CIP-004-6 R3 also should allow for CIP Exceptional Circumstances because the requirement to obtain a Personal Risk Assessment takes additional time that would hinder the ability of first responders to enter a Physical Security Perimeter in the event of the need for life saving measures. This would be consistent with CIP-004-3 "except in specified circumstances such as an emergency."
- *Impediment of large scale workforce availability*: CIP-007-6 R2 Security Patch Management requirements may be difficult to meet in the event that a major storm impacts a responsible entity, which requires all employees to report for storm duty for restoration efforts.
- *Natural disaster*: CIP-006-6 R1 Part 1.4 monitoring may not be possible if the physical access point to a PSP is under water or destroyed by a storm. Similarly, Part 1.3 causes compliance issues if for example, a fire renders a PACS controller panel inoperable and the PSP access points have failed secure. Emergency response may have to use a physical key, mechanical lock, or an axe to gain access. Without the IAC language or CIP Exceptional Circumstance provision, PSP access point monitoring is a zero defect issue.

We recommend that the SDT review all of the requirements of CIP V5 to determine whether: a CIP Exceptional Circumstances provision should be added, the definition of CIP Exceptional Circumstances should be edited, and/or additional explanatory language should be added to the Guidelines and Technical Basis for each standard regarding CIP Exceptional Circumstances.

Issue 2: BES Cyber Asset definition – "redundancy"

The application of the redundancy clause in the BES Cyber Asset (BCA) definition is unclear because the use of different and separate technologies and methods reduce reliability risk by providing alternative data sources. For example, VoIP systems, data center phone systems, radios, and other backup communication systems are alternatives, yet could be considered redundant by auditors and therefore it is unclear whether there are limits to the application of the BCA adverse impact to these systems. Without such limitations, the BCA definition may encourage registered entities to reduce their use of backup/alternative systems to reduce their compliance burdens and risk. While redundant assets may typically have identical security risks and vulnerabilities, requiring both/all to be similarly protected, alternative systems or assets are often substantially different and have drastically dissimilar risks and vulnerabilities, which reduces overall risk to the BES.

Issue 3: VoIP as a BES Cyber Asset

CIP-002-5.1 4.2.3.2 exempts "Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters" from CIP-002-5.1; however, the Guidelines and Technical Basis for CIP-002-5.1 calls out operational directives (TOP, RC, BA) as an aspect of Inter-Entity Coordination and Communication function. As a result, some auditors are viewing VoIP as in scope for CIP-002-5.1 despite the exemption and fact that different and separate communication technologies are used for this function. If the exemption does not apply, then the BES Cyber Asset definition should also apply; however, EEI members are hearing that auditors do not agree and believe that VoIP used for operational directives are BES Cyber Assets even if the 15 minute impact does not apply due to the redundancy issue mentioned above.

We recommend that the SDT consider these issues and determine how best to address VoIP in the standard that is aligned with the risk to the bulk electric system.

Issue 4: LERC definition application to assets located external to the low impact asset

The last three asset classes in CIP-002-5.1 R1 are typically implemented across multiple instances of the first three classes (i.e., systems and facilities critical to system restoration, special protection systems, and distribution provider protection systems are typically implemented at control centers, substations, and generating resources).

The Low Impact External Routable Connectivity (LERC) definition appears to be based on single asset locations ("direct user-initiated interactive access or a direct device-to-device connection to a low impact BES Cyber System(s) from a Cyber Asset ***outside the asset*** containing those low impact BES Cyber System(s) via a bi-directional routable protocol connection.") The phrase "outside the asset" can cause confusion in determining whether LERC exists for these classes of assets that are implemented across multiple sites.

For example, when evaluating a cranking path as an asset to determine if it has LERC, what does "outside the asset" mean? This could also allow for routable protocol based communication within the multiple substation cranking path to not be considered LERC and left unprotected if the entire cranking path is considered a single "asset containing low impact BES Cyber Systems." It appears these last 3 asset classes are actually criteria that should affect the categorization of the single site asset class where they are implemented.

Issue 5: Custom software (scripts)

CIP-010-2 R1, Part 1.1, subpart 1.1.3 requires a baseline configuration for "any custom software installed." The Guidelines and Technical Basis for this requirement states that "custom software installed may include scripts developed for local entity functions." It is unclear whether all scripts must be considered custom software or whether only scripts that can have an impact on the bulk electric system within 15 minutes must be considered custom software under this requirement. A risk-based clarification should be added to this requirement to set boundaries as to what is considered custom software. For example, a script that alters the behavior or function of a BES Cyber Asset or System should be included; however, a script that simply gathers log data, and whose only impact to the BES Cyber Asset is the allocation of incidental CPU cycles, need not be included.

Issue 6: Applicability of the requirement part to Cyber Asset vs. Cyber System

Some requirements such as in the CIP-007-6 standard apply to Cyber Assets within a BES Cyber System (e.g., the R2 security patch management requirements), others apply at either the BES Cyber System level or Cyber Asset level (e.g., the R4 Part 4.1 logging requirements), and others don't specific if they apply at the system or asset level (e.g., R3 Part 3.1 method to deter, detect, or prevent malicious code). Although the applicable systems for each of these requirements is generally the same (i.e., high and medium impact BES Cyber Systems and their associated EACMS, PACS, and PCA), the difference in the requirements language applicability to Cyber Assets, BES Cyber System, or both makes what is necessary to comply with the requirements unclear.

For example, the requirements section for CIP-007-6 R3 Part 3.1 does not specify whether this requirement applies at the BES Cyber System level or Cyber Asset level, therefore it is unclear whether a responsible entity can protect a medium impact BES Cyber System through deploying an anti-virus solution at the BES Cyber System level or whether the entity must deploy the solution at each Cyber Asset to comply with the requirement part. Consistency among the requirements language would be helpful in clearing up this confusion.

Issue 7: Control Center definition

The NERC document titled "CIP V5 Issues for Standard Drafting Team Consideration" already raises issues with the Control Center definition related to Transmission Owner Control Centers; however, it does not address issues related to Generator Operators.

By definition, a Control Center is "one or more facilities hosting operating personnel that monitor and control the Bulk Electric System (BES) in real-time to perform the reliability tasks, including their associated data centers … 4) a Generator Operator for generation Facilities at two or more locations."

Dispersed or distributed generation facilities (e.g., wind, solar, hydro) may not have the traditional control building with a horseshoe operator control desk ("facility hosting operating personnel that monitor and control"). Does the facility have to perform all "real-time … reliability tasks" or as few as one? Does a control room at a single wind farm, which controls a hundred turbines spread over many miles, meet the control center definition or does it become a control center only if it controls multiple wind farms? Also, if personnel maintains the Cyber Assets (e.g., patching or troubleshooting) is this considered "monitor and control" even though they are not personnel performing real-time reliability tasks. Does operating personnel mean those charged with the responsibility to monitor and control the BES or simply personnel who may be located at the generation Facility to maintain the equipment? Also, do each of the "generation Facilities at two or more locations" need to meet the Bulk Electric System definition to be within scope of the Control Center definition? CIP-002-5.1 Requirement R1, iii uses Generation resources, which could be interpreted to include all generation sources, even those that do not meet the Bulk Electric System definition.

As dispersed or distributed generation increases, clarity in language of the standard will become more important.

Issue 8: Security patches for operating Cyber Assets brought into scope under CIP V5

CIP-007-6 R2, Part 2.2 is clear concerning the ongoing evaluation of security patches as of July 1, 2016, but is unclear on what is required for the initial execution of the process ("evaluate security patches for applicability that have been released since the last evaluation") when there is no "last evaluation."

The standard does not require all Systems to be updated by July 1, 2016, but does require a baseline configuration, which includes a listing of all applied patches. The Guidelines and Technical Basis for CIP-010-2 states that "security patches applied would include all patches that have been applied on the cyber asset… CIP-010 Requirement R1, Part 1.1.5 requires entities to list all applied historical and current patches." This documentation requirement is particularly burdensome for an asset that has been in service for six years or longer as it requires entities to contact and work closely with their vendors to identify and get historical security patches. Also, documenting all historical patches, especially those that happened years ago will have little, if any impact on reliability.

Issue 9: Guidance for Secure Interactive Remote Access

In the Guidelines and Technical Basis for CIP-005-5, under Requirement R2 it states: “see Secure Remote Access Reference Document (see remote access alert).” Also, the Rationale for R2 states “Additional information is provided in Guidance for Secure Interactive Remote Access published by NERC in July 2011.” We believe these references are to the same document, which is properly titled under the Rationale and note that the 2011 NERC document was written in the context of V3 and not V5. Please evaluate the relevance of this guidance document to the most recent version (currently CIP-005-5). Also please clarify that IRA is intended to address access remotely from outside the organization (i.e., not to include accesses internally between protected networks).

Issue 10: Mistakes in Guidelines and Technical Basis

In implementing CIP V5, we’ve noticed a number of mistakes, which should be addressed, including:

- The rationale statements from the -5 standards were lost in several of the -6 versions of the standards. For example, the second sentence of the CIP-007-5 R2 rationale “The remediation plan can be updated as necessary to maintain the reliability of the BES, including an explanation of any rescheduling of the remediation actions.” was not carried forward to the -6 Guidelines and Technical Basis, even though there were no changes to the requirement between versions. We recommend reviewing the Rationales in the -6 standards and adding any that were deleted to the Guidelines and Technical Basis of the standard.
- For CIP-007-6 Part 2.2 the Guidelines and Technical Basis states: “Determination that a security related patch, hotfix, and/or update poses too great a risk to install on a system or is not applicable due to the system configuration should not require a TFE.” However there are no CIP-007-6 R2 Parts have TFE provisions.
- For CIP-004-6 R4, under the Guidelines and Technical Basis, the Rationale for this requirement states: “to ensure that individuals with access to BES Cyber Systems and the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity have been properly authorized for such access. “ ‘Authorization’ should be considered to be a grant of permission by a person or persons empowered by the Responsible Entity to perform such grants ***and included in the delegations referenced in CIP-003-6***” CIP V3 required designating approvers; however this requirement was not included in CIP-003-6 and therefore the emphasized text should be removed***.***
- For CIP-004-6 R4, the Rationale also references “quarterly reviews in Part 4.5”; however there is no Part 4.5 in CIP-004-6 R4.

Likes 0	
Dislikes 0	

Response

Jeri Freimuth - APS - Arizona Public Service Co. - 1,3,5,6

Answer	Yes
Document Name	

Comment

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 - Northeast Power Coordinating Council - 1,2,3,4,5,6 - NPCC, Group Name RSC No Dominion	
Answer	Yes
Document Name	
Comment	
Request that the SAR explicitly reference the correct title of the V5 TAG document, which we believe is “CIP V5 Issues for Standard Drafting Team Consideration, “dated on September 15, 2015.	
Likes 0	
Dislikes 0	
Response	
Chris Gowder - Florida Municipal Power Agency - 3,4,5,6 - FRCC, Group Name FMPA	
Answer	Yes
Document Name	
Comment	
Distribution Provider is not checked as an affected Reliability Function.	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	

Answer	
Document Name	4-15-16 DRAFT CIP V5 Implementation Issues.pdf
Comment	
Southern supports the comments of EEI. See attached.	
Likes 0	
Dislikes 0	
Response	

Comments received from Ginette Lacasse, Seattle City Light

Here are our Subject Matter Expert's (SME) comments. Non-italicized text is copied from SAR, with SME additions in RED. Additional SME comments are *in italics*.

Questions

1. **Do you agree with the scope and objectives of this SAR? If not, please explain why you do not agree, and, if possible, provide specific language revisions that would make it acceptable to you.**

Yes:
No: X

Comments:

In several sections the language of the SAR summarizes that of the foundation V5TAG document, but in doing so conflates or glosses over important concepts. Seattle City Light would like to see clarification to the SAR in the following two sections: (added text in red to clarify)

A) Cyber Asset and BES Cyber Asset (BCA) Definitions – as foundational definitions within the CIP V5 standards, the understanding of Cyber Asset and BCA terms impacts the scope of the applicable requirements. 'Right-sizing' the definitions of "Cyber Asset" and "BES Cyber Asset" balances between the administrative burden and negligible security benefit of an overly broad interpretation and the cyber security risk of too narrow an interpretation. The V5TAG recommends the following enhancements:

- Clarify the intent of “programmable” in Cyber Asset.
- Clarify and focus the definition of “BES Cyber Asset” including:
- Focusing the definition so that it does not subsume all other cyber asset types.
- Considering a lower bound to the term ‘adverse’ in “adverse impact”.
- Clarifying the double impact criteria (cyber asset affects a facility and that facility affects the reliable operation of the BES) such that “N-1 contingency” is not a valid methodology that can eliminate an entire site and all of its Cyber Assets from scope.

B) Network and Externally Accessible Devices – V5TAG recommends improving clarity within the concepts and requirements concerning Electronic Security Perimeters (ESP), External Routable Connectivity (ERC), and Interactive Remote Access (IRA) including:
   - The 4.2.3.2 exemption phrase “between discrete Electronic Security Perimeters.” When there is not an ESP at the location, consider clarity that the communication equipment considered out of scope is the same communication equipment that would be considered out of scope if it were between two ESPs.

2 Are you aware of any Canadian provincial or other regulatory requirements that may need to be considered during this project in order to develop a continent-wide approach to the standards? If yes, please identify the jurisdiction and specific regulatory requirements.

Yes:
No: X

Comments:

3 Are there any other concerns with this SAR that haven’t been covered in previous questions?

Yes: X
No:

Comments*:*

Seattle would like to see the SAR address three additional areas:

A) Clarify those standards and parts where the requirement applies solely to the applicable BES Cyber System, those standards and parts where the requirement applies solely to individual BES Cyber Assets, those where the requirement applies to both BCS and BCA or to either at the option of the responsible entity, and those where the requirement applies to both BCS and BCA or to either depending on the circumstances and configuration.

B) Clarify application of CIP-002-5, in particular the R1 identification of BES Cyber Systems and their association with specific types of assets (small “a”). The linkage is inconsistent: for High impact rating it is any “BCS located at and used by” a Control Center whereas for Medium

impact rating it is any "BCS associated with any of the following," the "following" being a mixed-bag collection of capital "F" Facilities, various systems or groups of Elements, specifically defined terms such as Control Center and Special Protection System, and undefined common-language concepts such as "generation" and "BES reactive resource." Please also clarify the intent of "used by" and "associated with." Does "used by" mean "essential to the operation of," "involved in the operation of," or something else? Does "associated with" combine the concepts of "used by and located at," or would it be sufficient to be either "situated at the physical location of" or "used by"? The present language creates considerable confusion.

C) *Clarify the application of Intermediate System, as discussed by Salt River Project in their comments. Seattle supports Salt River's position and analysis.*

Seattle also supports the position that Florida Municipal Power Authority as they submitted in their comments.

Comments received from Kara Douglas – NRG

Questions

1. Do you agree with the scope and objectives of this SAR? If not, please explain why you do not agree, and, if possible, provide specific language revisions that would make it acceptable to you.

   Yes:
   No: X
   Comments:

   A) Please consider the definition of Cyber Asset and clarify the intent of the term "Programmable" through consideration of whether a device is merely configurable, its executable code is not field upgradable or field Programmable, or if its functionality can only be changed via physical DIP switches, swapping internal chips, etc. (which relates to upgrading the executable in the Programmable code and the ability to field program the configuration)

   B) In relation to the terms: "adverse impact" and "control center", NRG proposes that when addressing TO and TOP Control Center functional obligations in CIP-002-5.1 Attachment 1, it also consider addressing similar issues facing Generator Owners (GO) and Generator Operators (GOP). There are GOP "control centers" that do not have traditional control capabilities over generator breakers or output but simply verbally direct generator actions. In this case it is the GOs that perform the actual output changes and breaker operation. Clarifying GO/GOP obligations in tandem with proposed TO/TOP clarification for determining impact is a step forward.

2. Are you aware of any Canadian provincial or other regulatory requirements that may need to be considered during this project in order to develop a continent-wide approach to the standards? If yes, please identify the jurisdiction and specific regulatory requirements.

Yes:
No: X
Comments:

3. Are there any other concerns with this SAR that haven't been covered in previous questions?

   Yes:
   No: X
   Comments:

Comments received from Marc Donaldson, Tacoma Power

1. Do you agree with the scope and objectives of this SAR? If not, please explain why you do not agree, and, if possible, provide specific language revisions that would make it acceptable to you.

   Yes:

   No: X

   Comments: Tacoma Power suggests the following scope changes:

   - 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.
   - SDT could provide clarity on CIP-002 eliminating ambiguous language ("Facility" vs. "facility" & "location") etc.
   - SDT should clarify whether CIP Exceptional Circumstance exception applies to CIP-004 R3 (PRA). Within the Guidelines and Technical Basis, there is this clarifier "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." We suggest the SDT include an exception for CIP Exceptional Circumstance specifically within the requirement language.

2. Are you aware of any Canadian provincial or other regulatory requirements that may need to be considered during this project in order to develop a continent-wide approach to the standards? If yes, please identify the jurisdiction and specific regulatory requirements.

   Yes:

No: X

Comments:

3. Are there any other concerns with this SAR that haven't been covered in previous questions?

   Yes:

   No: X

   Comments: