Exhibit A

Proposed Reliability Standard

CIP-012-1

A. Introduction

1. **Title:** Cyber Security – Communications between Control Centers
2. **Number:** CIP-012-1
3. **Purpose:** To protect the confidentiality and integrity of Real-time Assessment and Real-time monitoring data transmitted between Control Centers.
4. **Applicability:**
   - **4.1. Functional Entities:** The requirements in this standard apply to the following functional entities, referred to as "Responsible Entities," that own or operate a Control Center.
     - **4.1.1. Balancing Authority**
     - **4.1.2. Generator Operator**
     - **4.1.3. Generator Owner**
     - **4.1.4. Reliability Coordinator**
     - **4.1.5. Transmission Operator**
     - **4.1.6. Transmission Owner**
   - **4.2. Exemptions:** The following are exempt from Reliability Standard CIP-012-1:
     - **4.2.1.** Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.
     - **4.2.2.** The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.
     - **4.2.3.** A Control Center that transmits to another Control Center Real-time Assessment or Real-time monitoring data pertaining only to the generation resource or Transmission station or substation co-located with the transmitting Control Center.
5. **Effective Date:** See Implementation Plan for CIP-012-1.

B. Requirements and Measures

R1. The Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) to mitigate the risks posed by unauthorized disclosure and unauthorized modification of Real-time Assessment and Real-time monitoring data while being transmitted between any applicable Control Centers. The Responsible Entity is not required to include oral communications in its plan. The plan shall include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. Identification of security protection used to mitigate the risks posed by unauthorized disclosure and unauthorized modification of Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers;

1.2. Identification of where the Responsible Entity applied security protection for transmitting Real-time Assessment and Real-time monitoring data between Control Centers; and

1.3. If the Control Centers are owned or operated by different Responsible Entities, identification of the responsibilities of each Responsible Entity for applying security protection to the transmission of Real-time Assessment and Real-time monitoring data between those Control Centers.

M1. Evidence may include, but is not limited to, documented plan(s) that meet the security objective of Requirement R1 and documentation demonstrating the implementation of the plan(s).

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" (CEA) means NERC, the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- The Responsible Entities shall keep data or evidence of each Requirement in this Reliability Standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	N/A	The Responsible Entity documented its plan(s) but failed to include one of the applicable Parts of the plan as specified in Requirement R1.	The Responsible Entity documented its plan(s) but failed to include two of the applicable Parts of the plan as specified in Requirement R1.	The Responsible Entity failed to document plan(s) for Requirement R1; Or The Responsible Entity failed to implement any Part of its plan(s) for Requirement R1, except under CIP Exceptional Circumstances.

D. Regional Variances

None.

E. Associated Documents

Implementation Plan.

Technical Rationale for CIP-012-1.

Implementation Guidance.

Version History

Version	Date	Action	Change Tracking
1		Respond to FERC Order No. 822	New
1	August 16, 2018	Adopted by NERC Board of Trustees	
1	TBD	FERC Order approving CIP-012-1	

Exhibit B

Implementation Plan

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2016-02 Modifications to CIP Standards
Reliability Standard CIP-012-1

Applicable Standard

- Reliability Standard CIP-012-1 - Cyber Security – Communications between Control Centers

Requested Retirements

- None

Prerequisite Standard

These standard(s) or definitions must be approved before the Applicable Standard becomes effective:

- None

Applicable Entities

- Balancing Authority
- Generator Operator
- Generator Owner
- Reliability Coordinator
- Transmission Operator
- Transmission Owner

Effective Date

Reliability Standard CIP-012-1 - Cyber Security – Communications between Control Centers

Where approval by an applicable governmental authority is required, Reliability Standard CIP-012-1 shall become effective on the first day of the first calendar quarter that is twenty-four (24) calendar months after the effective date of the applicable governmental authority's order approving the standard, or as otherwise provided for by the applicable governmental authority.

Where approval by an applicable governmental authority is not required, Reliability Standard CIP-012-1 shall become effective on the first day of the first calendar quarter that is twenty-four (24) calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Exhibit D

Consideration of Directives

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Project 2016-02 Consideration of Issues and Directives

Federal Energy Regulatory Commission Order No. 822

August 2018

Directives from FERC Order No. 822		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
53	53. As discussed in detail below, however, the Commission concludes that modifications to CIP-006-6 to provide controls to protect, at a minimum, communication links and data communicated between bulk electric system Control Centers are necessary in light of the critical role Control Center communications play in maintaining bulk electric system reliability. Therefore, we adopt the NOPR proposal and direct that NERC, pursuant to section 215(d)(5) of the FPA, develop modifications to the CIP Reliability Standards to require responsible entities to implement controls to protect, at a minimum, communication links and sensitive bulk electric system data communicated between bulk electric system Control Centers in a manner that is appropriately tailored to address the risks posed to the bulk electric system by the assets being protected (i.e., high, medium, or low impact).	The Project 2016-02 Standard Drafting Team (SDT) drafted Reliability Standard CIP-012-1 Requirement R1 to require responsible entities to implement one or more documented plan(s) to mitigate the risks posed by unauthorized disclosure and unauthorized modification of Real-time Assessment and Real-time monitoring data while being transmitted between applicable Bulk Electric System (BES) Control Centers. Due to the sensitivity of the data being transmitted between the Control Centers, the SDT created the standard to apply to all impact levels of BES Cyber Systems (i.e., high, medium, or low impact). Based on operational risk, the SDT determined that Real-time Assessments and Real-time monitoring data was the appropriate scope of the requirement. This critical information is necessary for immediate situational awareness and real-time operation of the BES.

Directives from FERC Order No. 822		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
		The SDT has drafted the requirement allowing Responsible Entities the flexibility to apply protection to the communication links, the data, or both, consistent with their operational environments to satisfy the security objective of the Commission's directive FERC Order No. 822 specifically references CIP-006-6, which pertains to physical security controls. CIP-006-6, Requirement R1, Part 1.10 focuses on protecting the nonprogrammable communication components between Cyber Assets within the same ESP for medium and high impact BES Cyber Systems. The SDT asserts that most of the communications contemplated by FERC Order No. 822 are not within the same ESP, and, as such, CIP-006-6, Requirement R1, Part 1.10 would not be the appropriate location for this requirement.
54	54. NERC and other commenters recognize that inter-Control Center communications play a critical role in maintaining bulk electric system reliability by, among other things, helping to maintain situational awareness and reliable bulk electric system operations through timely and accurate communication between Control Centers.[59] We agree with this assessment. In order for certain responsible entities such as reliability coordinators, balancing authorities, and transmission operators to adequately perform their reliability	The SDT agrees that inter-Control Center communications play a critical role in Bulk Electric System reliability. Responsible Entities should therefore apply security measures to mitigate the risks posed by unauthorized disclosure and unauthorized modification of Real-time Assessment and Real-time monitoring data. Since the current CIP Reliability Standards do not address this, the SDT has designed the requirement to protect the data while it is being transmitted between inter-entity and intra-entity Control Centers.

Directives from FERC Order No. 822		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
	functions, their associated control centers must be capable of receiving and storing a variety of sensitive bulk electric system data from interconnected entities. Accordingly, we find that additional measures to protect both the integrity and availability of sensitive bulk electric system data are warranted.[60] We also understand that the attributes of the data managed by responsible entities could require different information protection controls. [61] For instance, certain types of reliability data will be sensitive to data manipulation type attacks, while other types of reliability data will be sensitive to eavesdropping type attacks aimed at collecting operational information (such as line and equipment ratings and impedances). NERC should consider the differing attributes of bulk electric system data as it assesses the development of appropriate controls. Footnotes: [59] NERC Comments at 20. [60] Protecting the integrity of bulk electric system data involves maintaining and ensuring the accuracy and consistency of inter-Control Center communications. Protecting the availability of bulk electric system data	The SDT has drafted a requirement that allows responsible entities to apply protection to the communication links, the data, or both to satisfy the security objective consistent with the capabilities of the responsible entity's operational environment.

Directives from FERC Order No. 822		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
	involves ensuring that required data is available when needed for bulk electric system operations. [61] Moreover, in order for certain responsible entities to adequately perform their Reliability Functions, the associated control centers must be capable of receiving and storing a variety of sensitive data as specified by the IRO and TOP Standards. For instance, pursuant to Reliability Standard TOP-003-3, Requirements R1, R3 and R5, a transmission operator must maintain a documented specification for data and distribute its data specification to entities that have data required by the transmission operator's Operational Planning Analyses, Real-time Monitoring and Real-time Assessments. Entities receiving a data specification must satisfy the obligation of the documented specification.	
55	55. With regard to NERC's development of modifications responsive to our directive, we agree with NERC and other commenters that NERC should have flexibility in the manner in which it addresses the Commission's directive. Likewise, we find reasonable the principles outlined by NERC that protections for communication links and sensitive bulk electric system data communicated between bulk electric system Control Centers: (1) should not have an adverse effect on reliability, including the recognition of instances where	The SDT drafted Reliability Standard CIP-012-1 to mitigate the risks posed by unauthorized disclosure and unauthorized modification of Real-time Assessments and Real-time monitoring data while being transmitted between Control Centers. The SDT developed an objective-based rather than prescriptive requirement. This approach will allow Responsible Entities flexibility in protecting these communications networks and sensitive BES data in a manner suited to each of their respective operational environments. It will also allow Responsible Entities to implement protection that considers the risks noted by the

Directives from FERC Order No. 822		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
	the introduction of latency could have negative results; (2) should account for the risk levels of assets and information being protected, and require protections that are commensurate with the risks presented; and (3) should be results-based in order to provide flexibility to account for the range of technologies and entities involved in bulk electric system communications.[62] Footnote: [62] See NERC Comments at 20-21.	Commission. The SDT identified a need to mitigate the risks posed by unauthorized disclosure and unauthorized modification of Real-time Assessment and Real-time monitoring data regardless of asset risk level. The proposal requires protection for all Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers.
56	56. We disagree with the assertion of NIPSCO and G&T Cooperatives that the risk posed by bulk electric system communication networks does not justify the costs of implementing controls. Communications between Control Centers over such networks are fundamental to the operations of the bulk electric system, and the record here does not persuade us that controls for such networks are not available at a reasonable cost (through encryption or otherwise). Nonetheless, we recognize that not all communication network components and data pose the same risk to bulk electric system reliability and may not require the same level of protection. We expect NERC to develop controls that reflect the risk posed by the asset or data being protected, and that can be implemented in	The SDT noted the FERC reference to additional Reliability Standards (TOP-003-3 and IRO-010-2) and the responsibilities to protect the data in accordance with those standards. The SDT interpreted these references as examples of potentially sensitive BES data and chose to base the CIP-012 requirements on the data specifications in TOP-003-3 and IRO-010-2. This consolidates scoping and helps ensure that Responsible Entities mitigate the risks posed by the unauthorized disclosure and unauthorized modification of Real-time Assessment and Real-time monitoring data, rather than leaving the scoping of sensitive bulk electric system data to individual Responsible Entities. The SDT drafted CIP-012-1 to address confidentiality and integrity of Real-time Assessment and Real-time monitoring

Directives from FERC Order No. 822		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
	a reasonable manner. It is important to recognize that certain entities are already required to exchange necessary real-time and operational planning data through secured networks using a "mutually agreeable security protocol," regardless of the entity's size or impact level.[63] 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. Footnote: [63] See Reliability Standards TOP-003-3, Requirement R5 and IRO-010-2, Requirement R3.	data. This was accomplished by drafting the requirement to mitigate the risks posed by unauthorized disclosure and unauthorized modification. The SDT asserts that the availability of this data is already required by the performance obligation of the TOP and IRO Reliability Standards. The SDT drafted CIP-012-1 to address the data while being transmitted. The SDT contends that this data is maintained within BES Cyber Systems, and is afforded the protection of CIP-003 through CIP-011 while at rest.
58	58. Several commenters sought clarification whether Control Centers owned by multiple registered entities would be included under the Commission's proposal. We clarify that the scope of the directed modifications apply to Control Center communications from facilities at all impact levels, regardless of ownership. The directed modification should encompass communication links and data for intra-Control Center and inter-Control Center communications.	The SDT drafted CIP-012-1 to apply to all impact levels of BES Cyber Systems (i.e., high, medium, or low impact), regardless of ownership. The SDT designed the requirement to mitigate the risks posed by unauthorized disclosure and unauthorized modification of Real-time Assessment and Real-time monitoring data while being transmitted between inter-entity and intra-entity BES Control Centers.

Directives from FERC Order No. 822		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
62	62. Several commenters addressed encryption and latency. Based on the record in this proceeding, it is reasonable to conclude that any lag in communication speed resulting from implementation of protections should only be measureable on the order of milliseconds and, therefore, will not adversely impact Control Center communications. Several commenters raise possible technical implementation difficulties with integrating encryption technologies into their current communications networks. Such technical issues should be considered by the standard drafting team when developing modifications in response to this directive, and may be resolved, e.g., by making certain aspects of the revised CIP Standards eligible for Technical Feasibility Exceptions.	The SDT developed an objective-based rather than prescriptive requirement. This approach will allow Responsible Entities flexibility in mitigating the risks posed by unauthorized disclosure and unauthorized modification of Real-time Assessments and Real-time monitoring data in a manner suited to each of their respective operational environments. It will also allow Responsible Entities to implement protection that considers the risks noted by the Commission.

Exhibit E

Implementation Guidance

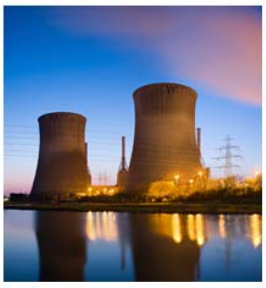
NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DRAFT Implementation Guidance
Pending Submittal for ERO Enterprise Endorsement

Cyber Security – Communications Between Control Centers

Implementation Guidance for CIP-012-1

RELIABILITY | ACCOUNTABILITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Introduction

The Project 2016-02 SDT drafted this Implementation Guidance to provide example approaches for compliance with CIP-012-1. Implementation Guidance does not prescribe the only approach, but highlights one or more approaches that would be effective in achieving compliance with the standard. Because Implementation Guidance only provides examples, entities may choose alternative approaches that better fit their individual situations[1].

Responsible Entities may find it useful to consider this Implementation Guidance document along with the additional context and background provided in the SDT-developed Technical Rationale and Justification for CIP-012-1 document.

Background

The Commission issued Order No. 822 on January 21, 2016. Order 822 approving seven CIP Reliability Standards and new or modified definitions, and directed modifications be made to the CIP Reliability Standards. Among other items, the Commission directed NERC to "develop modifications to the CIP Reliability Standards to require responsible entities to implement controls to protect, at a minimum, communication links and sensitive bulk electric system data communicated between bulk electric system Control Centers in a manner that is appropriately tailored to address the risks posed to the bulk electric system by the assets being protected (i.e., high, medium, or low impact)." (Order 822, Paragraph 53)

In response to the directive in Order No. 822, the Project 2016-02 standard drafting team (SDT) drafted Reliability Standard CIP-012-1 to require Responsible Entities to implement controls to protect sensitive Bulk Electric System (BES) data and communications links between BES Control Centers. Due to the sensitivity of the data being communicated between Control Centers, the standard applies to all impact levels (i.e., high, medium, or low impact).

The SDT drafted requirements to provide Responsible Entities the latitude to protect the communication links, the data, or both, to satisfy the security objective consistent with the capabilities of the Responsible Entity's operational environment.

[1] NERC's Compliance Guidance Policy

Requirements

R1. *The Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) to mitigate the risks posed by unauthorized disclosure and unauthorized modification of Real-time Assessment and Real-time monitoring data while being transmitted between any applicable Control Centers. The Responsible Entity is not required to include oral communications in its plan. The plan shall include: [Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. Identification of security protection used to mitigate the risks posed by unauthorized disclosure and unauthorized modification of Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers;

1.2. Identification of where the Responsible Entity applied security protection for transmitting Real-time Assessment and Real-time monitoring data between Control Centers; and

1.3. If the Control Centers are owned or operated by different Responsible Entities, identification of the responsibilities of each Responsible Entity for applying security protection to the transmission of Real-time Assessment and Real-time monitoring data between those Control Centers.

General Considerations

Plan Development

As noted in the Technical Rationale and Justification for CIP-012-1, the focus of Requirement R1 is implementing a documented plan to protect information that is critical to the real-time operations of the Bulk Electric System while in transit between applicable Control Centers. The number of plan(s) and their content may vary depending on a Responsible Entity's management structure and operating conditions. The Responsible Entity may document as many plans as necessary to meet its needs. For instance, a Responsible Entity may choose to document one plan per Control Center or choose an all-inclusive, single plan for its Control Center communication environment. A Responsible Entity may choose to document one plan for communications between Control Centers it owns and a separate plan for communications between its Control Centers and the Control Centers of a neighboring Entity. The number and structure of the plans is at the discretion of the Responsible Entity as long as the plan(s) include the required elements described in Parts 1.1, 1.2, and 1.3 of Requirement R1.

Identification of Real-time Assessment and Real-time monitoring data

Responsible Entities can expect to receive or have received requests for Operations Planning Analysis, Real-time Assessment and Real-time monitoring data from their RC(s), BA(s) and TOP(s). These data requests, pursuant to the data specification from TOP-003 and IRO-010 requirements, may also include other types of data under the same request. CIP-012 requires protection only for Real-time Assessment and Real-time monitoring data. If the provided data specification does not indicate which data is Real-time Assessment and Real-time monitoring data, Responsible Entities could choose to conduct an assessment to identify this data from among the other data requested or being communicated. Once a data assessment is completed, the Responsible Entity should confirm its findings with the other communicating entity before applying security controls. If the Real-time Assessment and Real-time monitoring data is not clearly identified in the provided data specification, the Responsible Entity should document the methodology used and all actions taken to identify the Real-time Assessment and Real-time monitoring data.

Identification of Security Protection

Entities have latitude to identify and choose which security protection is used to mitigate the risks posed by unauthorized disclosure and unauthorized modification of Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers.

This security protection could consist of logical protection, physical protection, or some combination of both. To determine security protection, the requirement specifies that it must mitigate the risks posed by unauthorized disclosure and unauthorized modification of applicable data.

Security protection implementation can be demonstrated in many ways. If a Responsible Entity uses physical protection, it may demonstrate implementation through review of an applicable Control Center floor plan with details subsequently confirmed through visual inspection, which identifies the physical security measures in place protecting the communication link. If the Responsible Entity uses logical protection, it may demonstrate implementation through an export of the device configuration which applies the security protection. Alternatively, a Responsible Entity may demonstrate implementation through security control monitoring, using an automated monitoring tool to generate reports on the encryption service used to protect a communications link. Where the operational obligations of an entire communication link, including both endpoints, belong to the Control Center of another Responsible Entity, the Responsible Entity without operational obligations for the communication link may demonstrate compliance by ensuring the communications link endpoint is within its Control Center, which could be limited to including the communication link endpoint within a PSP or where other physical protection is applied.

Identification of Where Security Protection is Applied by the Responsible Entity

A Responsible Entity should consider its environment when identifying where security protections should be applied. One approach is to implement security within the Control Center itself to ensure that data confidentiality and integrity is protected throughout the transmission. The Responsible Entity can identify where security protection is applied using a logical or physical location The application of security in accordance with CIP-012 requirements does not add additional assets to the scope of the CIP Reliability Standards. Locations of applied security protection may vary based on many factors such as impact levels of the Control Center, different technologies, or infrastructures. Where the operational obligations of an entire communication link, including both endpoints, belong to the Control Center of another Responsible Entity, the Responsible Entity without operational obligations for the communication link may demonstrate compliance by ensuring the communications link endpoint is within its Control Center, which could be limited to including the communication link endpoint within a PSP or where other physical protection is applied.

Identification of where a Responsible Entity applies security protection could be demonstrated with a list or a Control Center diagram showing either physical or logical security controls. Physical diagrams may require visual confirmation of these controls. These diagrams or a list could be included within the plan developed for R1. A Responsible Entity could also use labels to identify on-site devices where CIP-012 security protection is applied.

When exchanging data between two entities, if a Responsible Entity only manages one end of a communication link, the Responsible Entity is not responsible for identifying where the security protection is applied by the neighboring entity with which it is exchanging data. However, if a Responsible Entity has taken responsibility for both ends of the communication link (such as by placing a router within the neighboring entity's data center), then the Responsible Entity shall identify where the security protection is applied at both ends of the link.

Similarly, if a Responsible Entity owns and operates both Control Centers which are exchanging data (such as in the case of a primary and backup Control Center), then the Responsible Entity shall identify where security protection is applied at both ends of the link.

Identification of Responsibilities when the Control Centers are Owned or Operated by Different Responsible Entities

The Technical Rationale and Justification for CIP-012-1 identifies key considerations in the Control Center Ownership section when communications between Control Centers with different owners or operators. Many operational relationships between Responsible Entities are unique. Consequently, there is no single way to identify responsibilities for applying security protection to the transmission of Real-time Assessment and Real-time monitoring data between Control Centers.

Implementation of responsibilities could also be demonstrated in many ways. Some examples include a joint procedure, a memorandum of understanding, or meeting minutes between the two parties where responsibilities are defined. These responsibilities should be included in both Responsible Entities' plans satisfying requirement Part 1.3.

Where the operational obligations of an entire communication link, including both endpoints, belong to the Control Center of another Responsible Entity, the Responsible Entity without operational obligations for the communication link may demonstrate compliance by ensuring the communications link endpoint is within its Control Center, which could be limited to including the communication link endpoint within a PSP or where other physical protection is applied.

Reference Model

For this Implementation Guidance, the SDT uses a basic reference model of Primary and Backup Control Centers (Entity Alpha) to illustrate approaches to demonstrating compliance. These Control Centers communicate to each other and to a neighboring entity's Control Center (Entity Beta) in configurations outlined by the diagrams in this section. The SDT recognizes that the reference model does not contain many of the complexities of a real Control Center. For this Implementation Guidance, the registration or functions performed in the reference model Control Center are also not considered. A high level block diagram of the basic reference model is shown below in Figure 1. This Implementation Guidance is developed from the perspective of Entity Alpha.

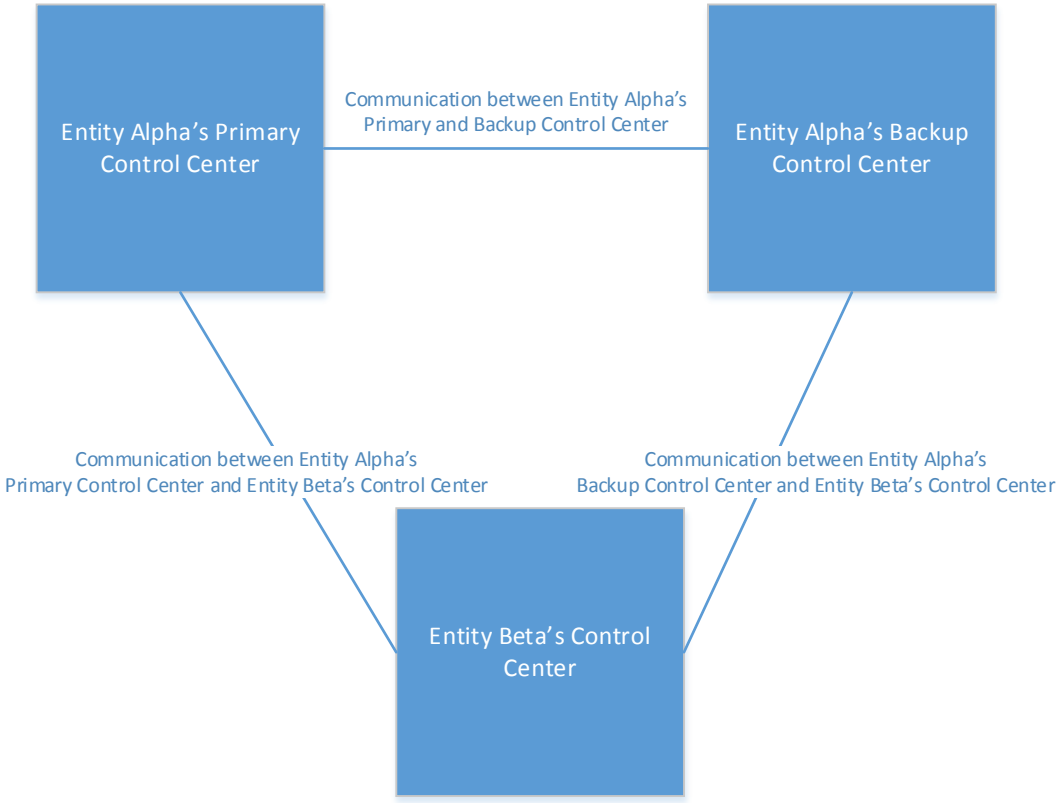


Figure 1: High Level Block Diagram of Reference Model Control Centers

Reference Model Discussion

Requirement R1 requires the implementation of a documented plan. To comply with requirement R1, one approach to a plan is to first determine which communications are in scope of CIP-012-1. There are multiple ways to identify an entity's scope in R1. For example, Entity Alpha in the reference model may first identify the Control Centers with which it communicates. Entity Alpha would determine that there are three: Entity Alpha's Primary Control Center, Entity Alpha's Backup Control Center, and Entity Beta's Control Center. Entity Alpha does not need to consider whether Entity Beta further shares its data with another Entity. That is the responsibility of Entity Beta and is outside of Entity Alpha's purview. Additionally, Entity Alpha does not need to consider any communications to other non-Control Center facilities such as generating plants or substations. These communications are out of scope for CIP-012-1.

Now that Entity Alpha has identified the Control Centers with which it communicates, Entity Alpha identifies either: (1) the Real-time Assessment and Real-time monitoring data; or (2) communication links which are used to transmit Real-time Assessment and Real-time monitoring data between Control Centers. In either case, Entity Alpha should refer to the data specification for Real-time Assessment and Real-time monitoring data identified in

TOP-003-3 and IRO-010-2. For this reference model scenario, identifying the communication links used to transmit Real-time Assessment and Real-time monitoring data may be the most straightforward approach. Through an evaluation of communication links between Control Centers and an evaluation of how it transmits and receives Real-time Assessment and Real-time monitoring data, Entity Alpha determined that it communicates applicable data between its primary and backup Control Centers across a single communication link. Entity Alpha also determined that it communicates applicable data to and from Entity Beta's Control Center across one of two links that originate from either Entity Alpha's primary or backup Control Center using the Inter-Control Center Communications Protocol (ICCP).

With an identified scope of communications links, Entity Alpha now considers the three required elements of its required communications between Control Centers for its plan.

Identification of Security Protection

- Entity Alpha must ensure that protection is applied where identified in its CIP-012-1 plan. The protection must also meet the security objective of mitigating the risks posed by unauthorized disclosure and unauthorized modification of applicable data while in transit between Control Centers. The identification of security protection could be demonstrated by a network diagram similar to that shown in Figure 2 or Figure 3.
- In a simple case where the security protection is applied sufficiently close to the Control Center, such as within the Physical Security Perimeter of the Control Center, Entity Alpha may use a single security protection method to meet the security objective. For this case, shown in Figure 2, Entity Alpha implements a Virtual Private Network (VPN) connection across a private leased communication circuit for each of its three in-scope communication links. To meet the security objective, Entity Alpha further states that its VPN uses Internet Protocol security (IPsec) with encryption.
- For more complex scenarios, Entity Alpha may need to use a combination of security controls. For instance, in Figure 3, Entity Alpha uses a combination of physical security controls (physical access control) and logical security controls (encrypted communications consistent with the first scenario above) to meet the security objective. The SDT notes that the same technical architecture could exist where the responsibilities of the registered entities are different. Therefore as shown in Figure 2 & 3, in the scenario where entity Alpha owns and operationally manages the communication link and endpoint equipment, Entity Beta is responsible for ensuring the communication endpoint of the communication link is within a Control Center. Entity Beta ensures Entity Alpha's communication link endpoint equipment is within a Control Center by including the communication endpoint within a Control Center PSP. The physical controls for the PSP are described in CIP-006 documentation and do not need to be repeated for this requirement. This satisfies Entity Beta's obligation for Part 1.1 and 1.2.
- While these scenarios are all specific to communication links, it is possible that Entity Alpha and Entity Beta achieve the security objective by applying protection to the data rather than the communication links. In this scenario, the application enabling the data exchange between Control Centers may be capable of applying security controls directly to the data. These security controls mitigate the risks posed by unauthorized disclosure and unauthorized modification of applicable data rather than relying on lower level network services to provide this security. For instance, Entity Alpha and Entity Beta may apply security protection at the application layer by using Secure ICCP to exchange applicable data. According to a report released by Sandia National Labs[2], Secure ICCP provides "data integrity indirectly by providing a cryptographic checksum. Secure ICCP provides data confidentiality by encrypting ICCP data exchanges." Methods other than Secure ICCP could also be used to apply security protection to the data at the application layer.

[2] https://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/19-Secure_ICCP_Integration.pdf

Identification of Where Security Protection is Applied by the Responsible Entity

Similar to the identification of security protection above, the identification of where security protection is applied can also be demonstrated by a network diagram similar to those found in Figures 2 and 3.

- Figure 2 shows the identification where CIP-012-1 security protection is applied for the Entity Alpha reference model when a single encrypted tunnel is used to implement the required protection. Entity Alpha has identified that security protection is applied at each of its Control Centers on the external Ethernet interface on the WAN router. While the diagram depicts where Entity Beta has applied security protection for illustrative purposes, Entity Alpha is not responsible for identifying where Entity Beta has applied security protection.
- In order to understand the application of security protection in context of who controls the communication link, it may be helpful to identify both where CIP-012-1 security protection is applied and the location of the telecommunications carrier (telco) demarcation point. Figure 3 provides such an example where the telco demarcation point may not be within the Control Center and based the facts and circumstances surrounding this scenario, Entity Alpha has implemented a combination of security controls to comply with CIP-012-1. In this scenario, Entity Alpha identifies that it has applied physical security protection for its PSP and continuing for its WAN router and that it has applied logical security protection (encryption) at the WAN router. Entity Alpha has also identified the telco demarcation point at a point in the telecommunications cabling connecting to Entity Alpha's WAN router, perhaps at a punch down block for example. In Figure 3, the telco demarcation point is inside the same room as the WAN router. The telco demarcation points are referenced in the drawing for clarity, but are not part of the plan.
- Figures 2 & 3 provide an example of where the operational obligations of an entire communications link, including both endpoints, belong to Entity Alpha. In this case, Entity Beta may be responsible for ensuring the communications endpoint of the communications link is within their Control Center. Entity Beta ensures Entity Alpha's communication link endpoint equipment is within a Control Center by including the communication endpoint within a Control Center PSP. The documentation provided for Part 1.1 by Entity Beta fulfils this obligation.
- The data-centric scenario described above is less intuitive for identifying where security protection is applied by Entity Alpha. If security protection is applied at the application layer (such as Secure ICCP), Entity Alpha could reasonably identify the application or service applying the security (such as the Secure ICCP service) as the location of where security protection is applied.

Identification of Responsibilities when the Control Centers are Owned or Operated by Different Responsible Entities

Entity Alpha and Entity Beta may determine they each are responsible for one end of the VPN configuration on their respective WAN routers. Entity Alpha and Entity Beta have agreed to a 30 character pre-shared key for IPSec authentication.

Rather than use a pre-shared key, Entity Alpha and Entity Beta may decide to use digital certificates for the IPSec authentication using a trusted certificate authority. In that scenario, Entity Alpha and Entity Beta would agree on who is the party responsible for managing the certificate authority.

In the example where the communication link and endpoint equipment are owned by Entity Alpha, both entities should include ownership responsibilities in their plans satisfying requirement 1.3. Examples include but are not limited to, a letter indicating ownership or responsibility, a copy of a contract indicating ownership or responsibilities, an excerpt from an operational agreement or manual indicating ownership or responsibility.

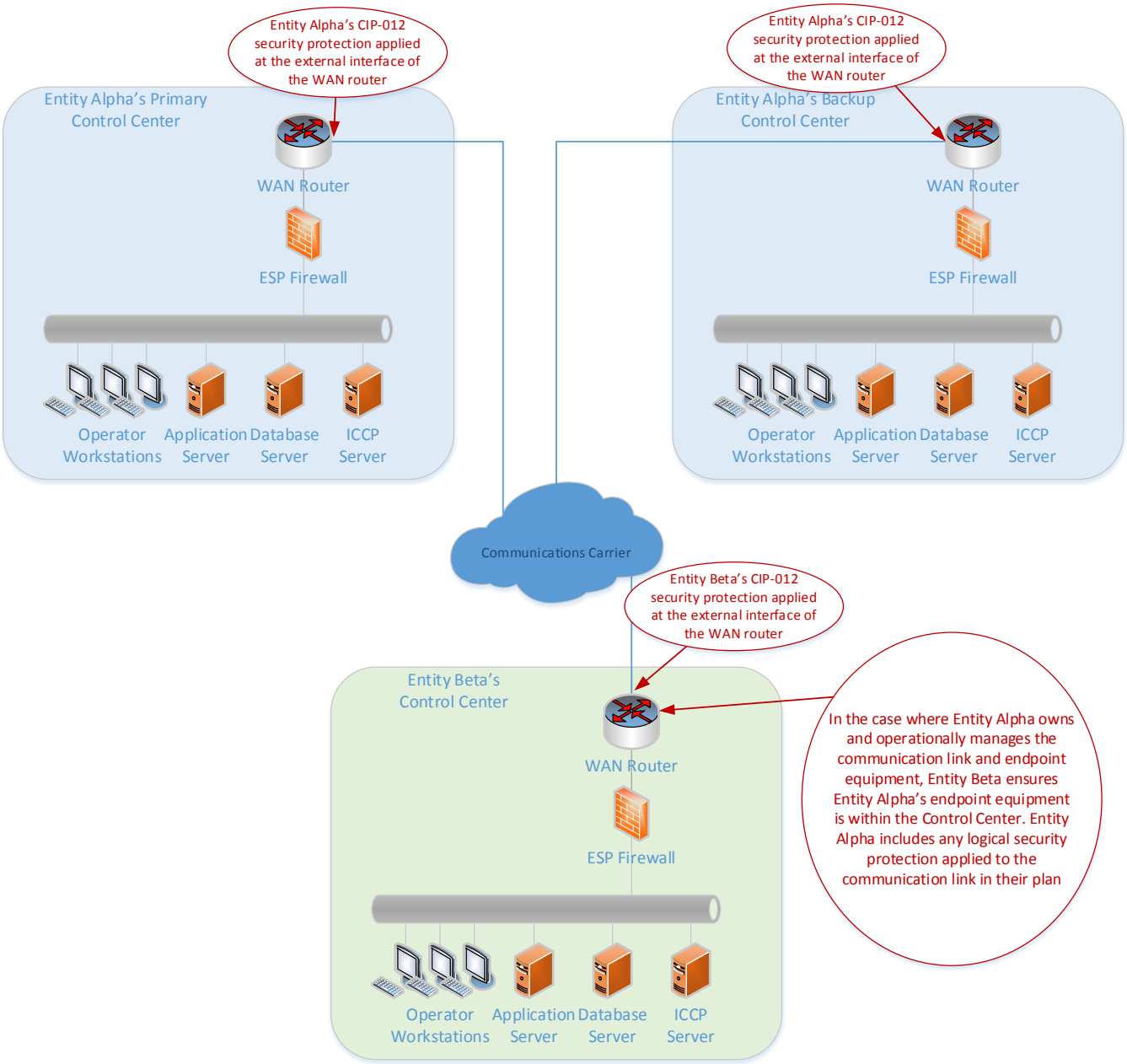


Figure 2: Network diagram and identification of where security protection is applied

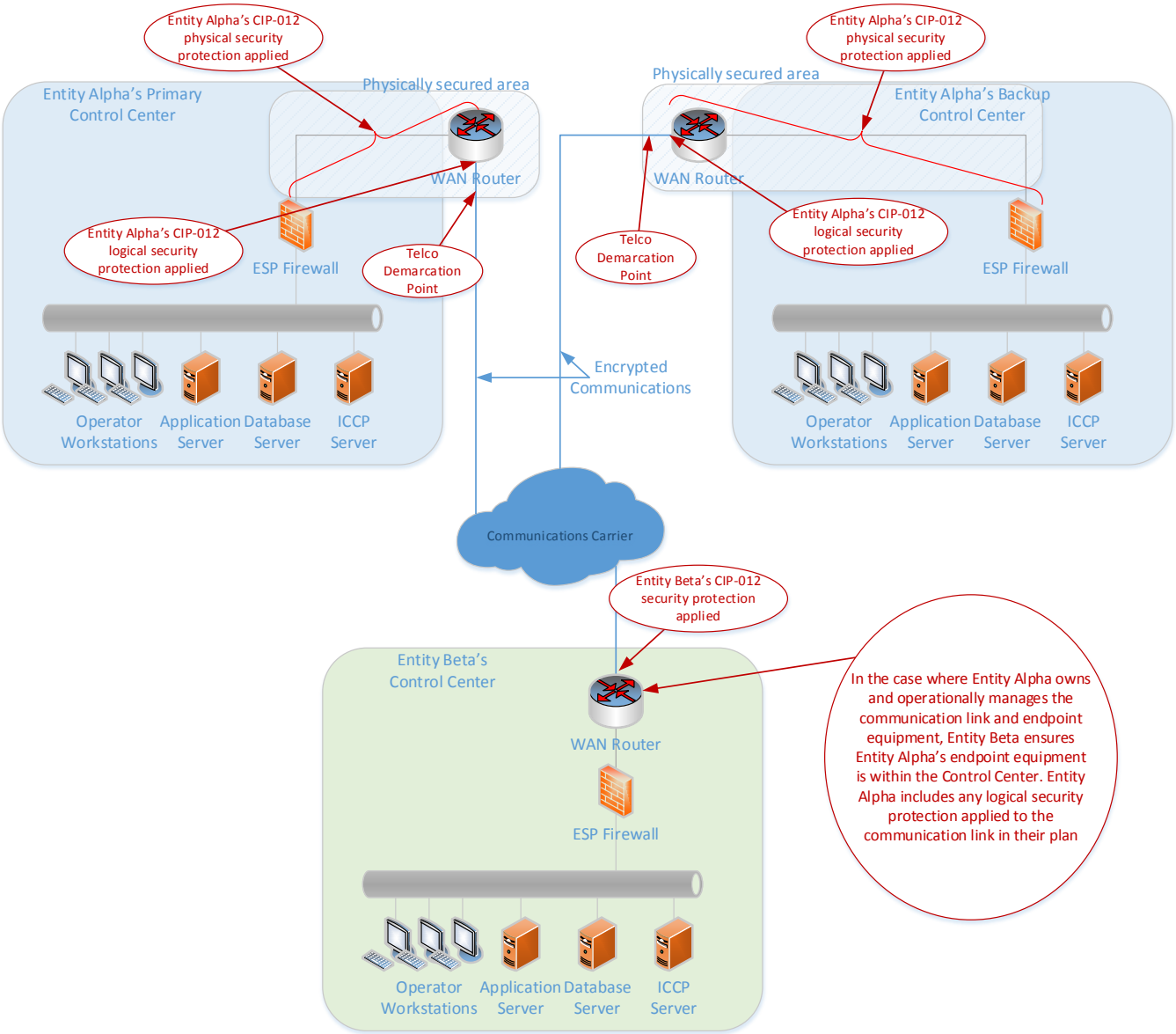


Figure 3: Network diagram using a combination of controls for CIP-012-1

References

Mitre Common Weakness Enumeration (CWE™) list of software weakness types
https://cwe.mitre.org/data/definitions/327.html

Cryptographic Standards and Guidelines
https://csrc.nist.gov/Projects/Cryptographic-Standards-and-Guidelines

NIST Special Publication 800-175B
Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-175B.pdf

Guide to Cryptography
https://www.owasp.org/index.php/Guide_to_Cryptography#Symmetric_Cryptography

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber Security – Communications between Control Centers

Technical Rationale and Justification for Reliability Standard CIP-012-1

RELIABILITY | ACCOUNTABILITY



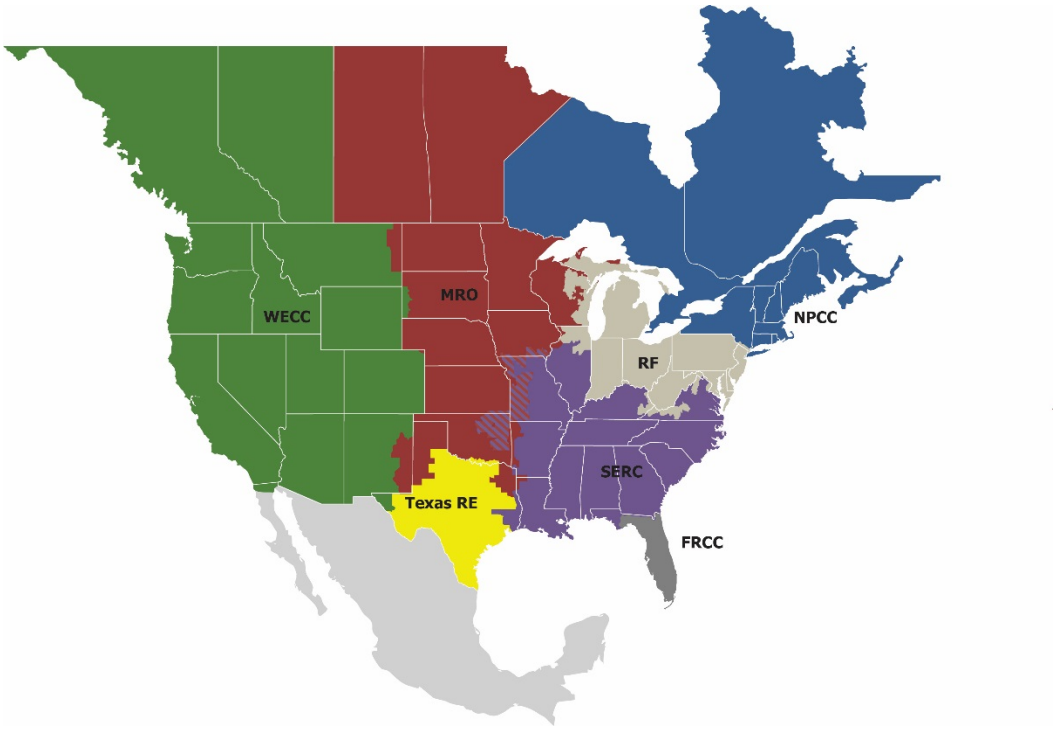

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Preface

The vision for the Electric Reliability Organization (ERO) Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the seven Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

The North American BPS is divided into seven RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.



FRCC	Florida Reliability Coordinating Council
MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-012-1. It will provide stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. It also contains information on the SDT's intent in drafting the requirements. This Technical Rationale and Justification for CIP-012-1 is not a Reliability Standard and should not be considered mandatory and enforceable.

On January 21, 2016, the Federal Energy Regulatory Commission (FERC or Commission) issued Order No. 822, approving seven Critical Infrastructure Protection (CIP) Reliability Standards and new or modified terms in the Glossary of Terms Used in NERC Reliability Standards, and directing modifications to the CIP Reliability Standards. Among others, the Commission directed the North American Electric Reliability Corporation (NERC) to "develop modifications to the CIP Reliability Standards to require Responsible Entities[1] to implement controls to protect, at a minimum, communication links and sensitive bulk electric system data communicated between bulk electric system Control Centers in a manner that is appropriately tailored to address the risks posed to the bulk electric system by the assets being protected (i.e., high, medium, or low impact)." (Order 822, Paragraph 53)

In response to the directive in Order No. 822, the Project 2016-02 standard drafting team (SDT) drafted Reliability Standard CIP-012-1 to require Responsible Entities to implement controls to protect sensitive Bulk Electric System (BES) data and communications links between BES Control Centers. Due to the sensitivity of the data being communicated between Control Centers, as defined in the Glossary of Terms Used in NERC Reliability Standards, the standard applies to all impact levels (i.e., high, medium, or low impact).

Although the Commission directed NERC to develop modifications to CIP-006, the SDT determined that modifications to CIP-006 would not be appropriate. There are differences between the plan(s) required to be developed and implemented for CIP-012-1 and the protection required in CIP-006-6 Requirement R1 Part 1.10. CIP-012-1 Requirements R1 and R2 protect the applicable data during transmission between two separate Control Centers. CIP-006-6 Requirement R1 Part 1.10 protects nonprogrammable communication components within an Electronic Security Perimeter (ESP) but outside of a Physical Security Perimeter (PSP). The transmission of applicable data between Control Centers takes place outside of an ESP. Therefore, the protection contained in CIP-006-6 Requirement R1 Part 1.10 does not apply.

The SDT drafted requirements to provide Responsible Entities the latitude to protect the communication links, the data, or both to satisfy the security objective consistent with the capabilities of the Responsible Entity's operational environment.

CIP-012 Exemption (4.2.3) for certain Control Centers

In the process of drafting CIP-012, the SDT became aware of certain generating plant or Transmission substation situations where such field assets could be dual-classified as Control Centers based on the current Control Center definition. Their communications to their BA or TOP Control Centers, however, are not included in the intended scope of CIP-012. This is because the communications do not differ from those of any other generating plant or substation. The SDT wrote an exemption (Section 4.2.3 within CIP-012) for this particular scenario which is described in further detail below.

I

[1] As used in the CIP Standards, a Responsible Entity refers to the registered entities subject to the CIP Standards.

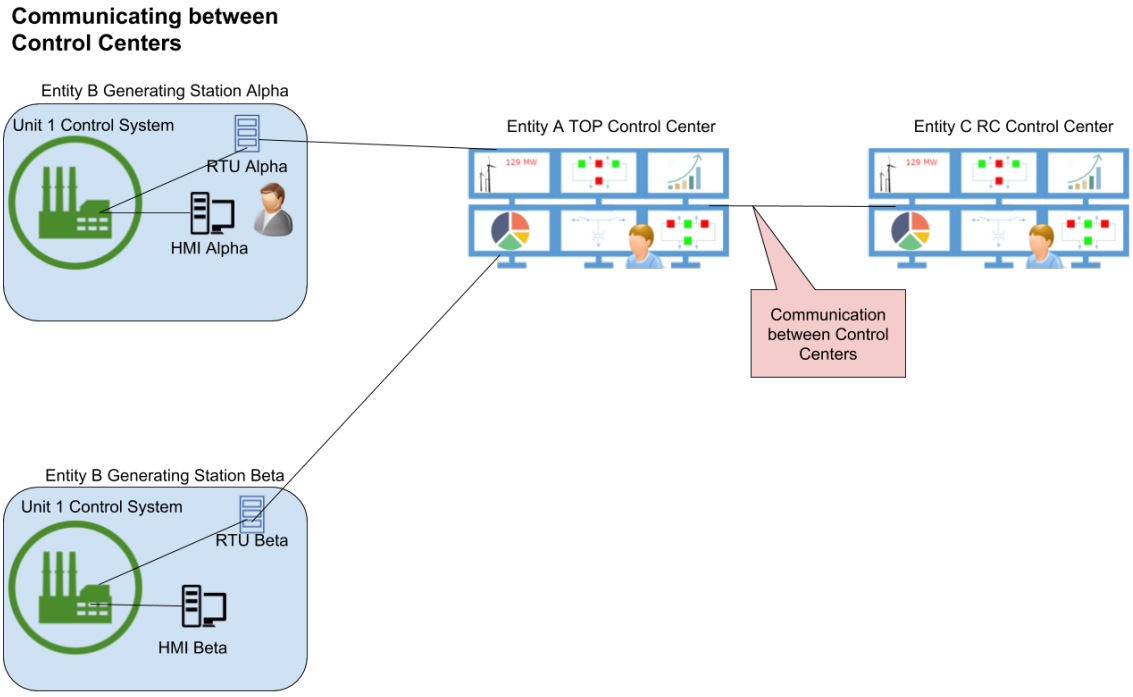


Figure 1

Figure 1 presents a typical scenario with two Control Centers communicating (in this instance Entity C's RC Control Center and Entity A's TOP Control Center). The communication between them is the intended scope of CIP-012's requirements if they meet the types of data inclusions and exclusions within the standard. The TOP Control Center is communicating with an RTU at two of Entity B's generating plants (Stations Alpha and Beta). Those RTU's are gathering information from each generating unit's control system. Each generating unit at each plant has an HMI (Human/Machine Interface; an operator workstation) that the local personnel use to operate their respective units.

Entity B decides that the generating unit at Station Beta, a small peaking facility, will only have an operator on site during the day. The operator at Station Alpha should be able to remotely start the unit at

Station Beta if necessary.

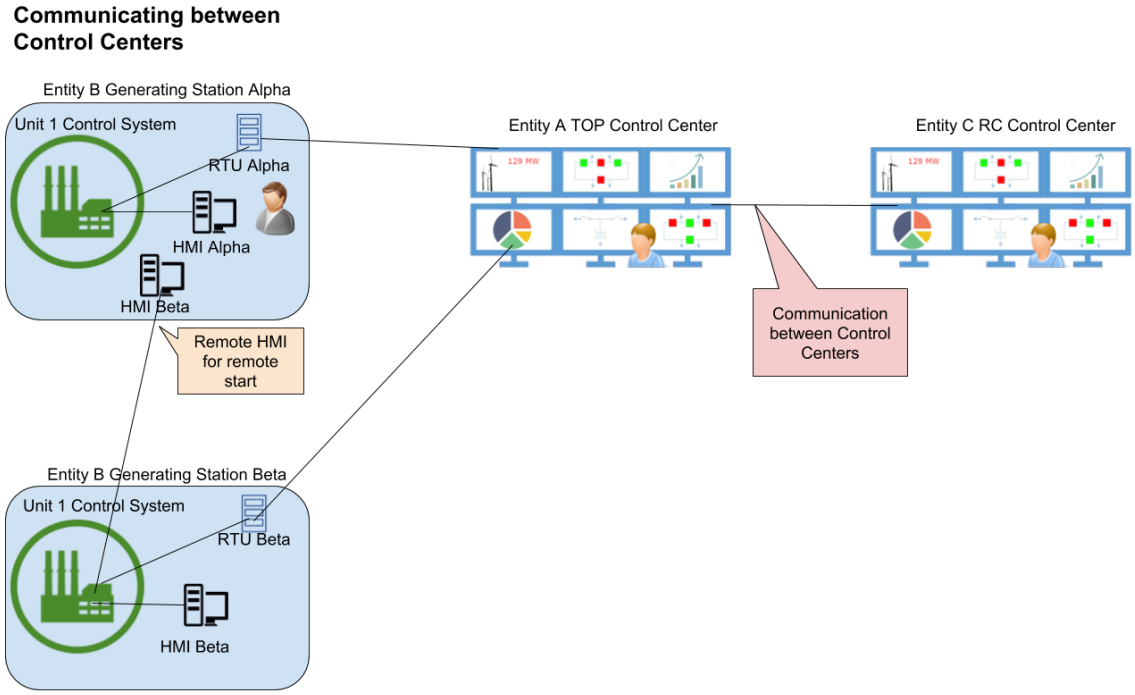


Figure 2

In Figure 2, Entity B installs a dedicated communications circuit from the control system on Station Beta's control system and puts a dedicated HMI at Station Alpha operator use. Station Alpha is now "one or more facilities hosting operating personnel that monitor and control the BES in real time to perform the reliability tasks of…a Generator Operator for generation Facilities at two or more locations" Because stations Alpha and Beta are two different plant locations. Station Alpha can now be dual-classified not only as a generation resource but also as a Control Center.

The communications to the TOP and RC Control Centers in Figure 1 have not changed. No new cyber systems are in place that can impact multiple units. In addition, no cyber systems have been added performing Control Center functions. The only change is that an HMI for Station Beta has been moved within close physical proximity to an HMI for Station Alpha.

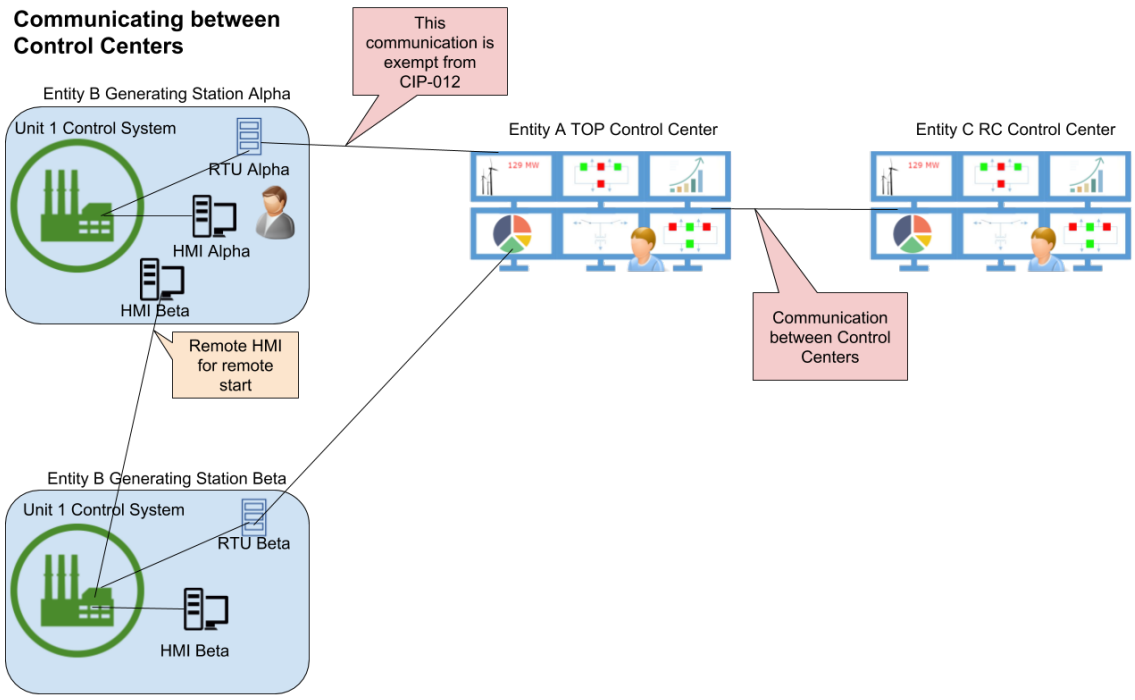


Figure 3

Although nothing has changed between them, this proximity makes the communication noted in Figure 3 between Station Alpha and Entity A's TOP Control Center subject to CIP-012 without the exemption. Two HMIs have been moved into the same room and a new NERC CIP standard applies to two entities.

This is an anomaly of the current Control Center definition of a facility, room, or building from which certain functions can be performed without regard to how they are done or what systems they are using. This is a generation specific example, but the potential situation exists where there are substations with an HMI or protective relay that "operating personnel" within the substation could use to impact an adjacent substation. It is also clear that in the criteria for TO's and GOP's the "two or more locations" is not a precise enough filter for defining what a Control Center truly is. The SDT's attempts to address this issue by clarifying the definition of Control Center pointed out larger issues that are not within the SDT's SAR to address at this time. Accordingly, the SDT is handling the issue through the 4.2.3 exemption within the CIP-012 standard which reads:

4.2.3. A Control Center g that transmits to another Control Center the transmitting Control Center.

The intent of this exemption is to exclude from CIP-012 the normal RTU-style communication from a field asset providing that field asset's status. Throughout this scenario or others like it, that communication has not changed and is still the same data pertaining only to the single location. The SDT recognizes that this communication is not the intent of the standard for protecting communications between Control Centers and this type of communications can be using older legacy communication technology and protocols.

The 4.2.3 exemption covers generation resources or Transmission station or substation locations that host operating personnel and can control BES Facilities at more than one location, possibly making them co-located Control Centers. The communication is exempt if each location is communicating the Real-time Assessment or Real-time monitoring data with another Control Center pertaining only to that location.

The above diagrams were generation specific. The following diagram is a more generic example:

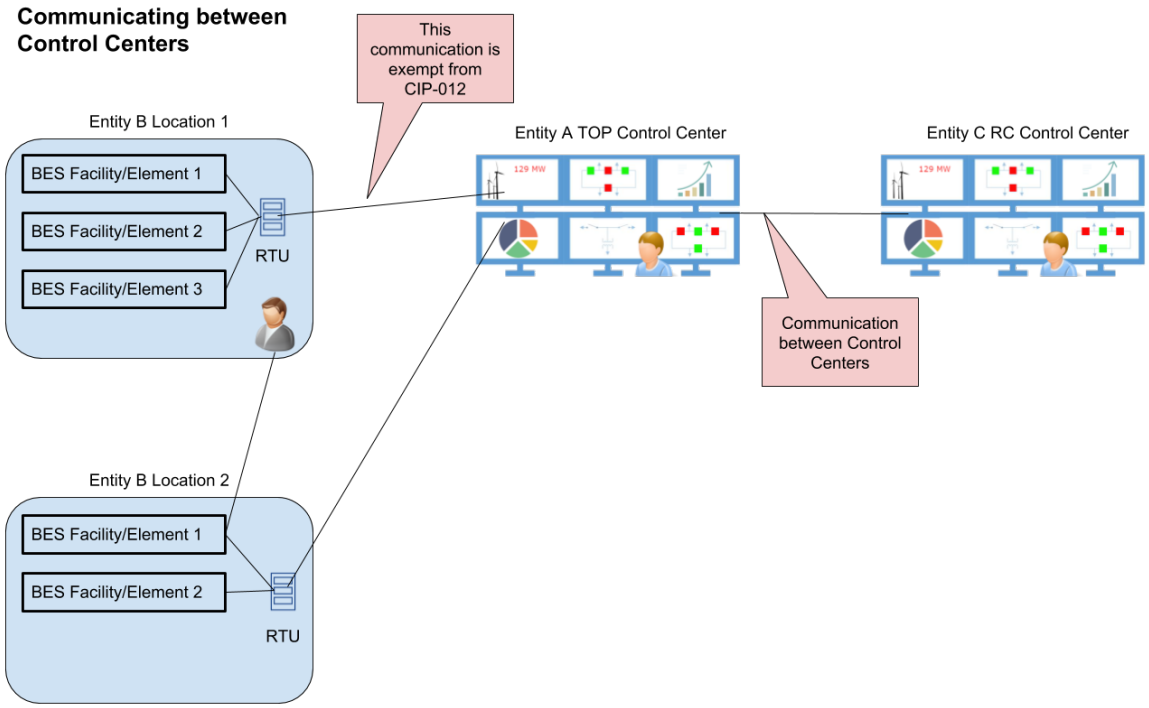


Figure 4

In Figure 4, each location is communicating only the Real-time Assessment or Real-time monitoring data pertaining to that single location. The communication from Entity B location one (1) to Entity A would be exempt from CIP-012-1.

If Location 2 communicates its data through Location 1,and Location 1 was both controlling and aggregating data from multiple locations to Entity A's TOP Control Center, the communication between Location 1 and Entity A's TOP Control Center would not be exempt from CIP-012.

Requirement R1

R1. The Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) to mitigate the risks posed by unauthorized disclosure and unauthorized modification of Real-time Assessment and Real-time monitoring data while being transmitted between any applicable Control Centers. The Responsible Entity is not required to include oral communications in its plan. The plan shall include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1 *Identification of security protection used to mitigate the risks posed by unauthorized disclosure and unauthorized modification of Real-time Assessment and Real-time monitoring while being transmitted between Control Centers;*

1.2 *Identification of where the Responsible Entity applied security protection for transmitting Real-time Assessment and Real-time monitoring data between Control Centers; and*

1.3 *If the Control Centers are owned or operated by different Responsible Entities, identification of the responsibilities of each Responsible Entity for applying security protection to the transmission of Real-time Assessment and Real-time monitoring data between those Control Centers.*

General Considerations for Requirement R1

Requirement R1 focuses on implementing a documented plan to protect information that is critical to the Real-time operations of the Bulk Electric System while in transit between applicable Control Centers. The SDT does not intend for the listed order of the three requirement parts to convey any sequence or significance.

Overview of confidentiality and integrity

The SDT drafted CIP-012-1 to address confidentiality and integrity of Real-time Assessment and Real-time monitoring data. This is accomplished by drafting the requirement to mitigate the risks posed by unauthorized disclosure (confidentiality) and unauthorized modification (integrity). For this Standard, the SDT relied on the definitions of confidentiality and integrity as defined by National Institute of Standards and Technology (NIST):

- Confidentiality is defined as, "Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information."[2]
- Integrity is defined as, "Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity."[3]

The SDT asserts that the availability of this data is already required by the performance obligation of the Operating and Planning Reliability Standards. The SDT drafted CIP-012-1 to address the data while being transmitted. The SDT maintains that this data resides within BES Cyber Systems, and while at rest is protected by CIP-003-6 through CIP-011-2.

Alignment with IRO and TOP standards

The SDT recognized the FERC reference to additional Reliability Standards and the responsibilities to protect the applicable data in accordance with NERC Reliability Standards TOP-003 and IRO-010. The SDT used these references to drive the identification of sensitive BES data and chose to base the CIP-012-1 requirements on the Real-time data

[2] NIST Special Publication 800-53A, Revision 4, page B-3
[3] NIST Special Publication 800-53A, Revision 4, page B-6

specification elements in these standards. This approach provides consistent scoping of identified data, and does not require each entity to devise its own list or inventory of this data. Many entities are required to provide this data under agreements executed with their RC, BA or TOP. Data requiring protection in CIP-012-1 consists of a subset of data that is identified by the RC, BA, and TOP in the TOP-003 and IRO-010 data specification standards, limited to Real-time Assessment data and Real-time monitoring data. CIP-012-1 excludes other data typically transferred between Control Centers such as Operational Planning Analysis data, weather data, market data, and other data that is not used by the RC, BA, and TOP to perform Real-time reliability assessments and analysis identified in TOP-003 and IRO-010. The SDT determined that Operational Planning Analysis data, if rendered unavailable, degraded, or misused, would not adversely impact the reliable operation of the BES within 15 minutes of the activation or exercise of the compromise as detailed in CIP-002- 5.1a. The SDT notes that there may be special instances during which Real-time Assessment or Real-time monitoring data is not identified by the RC, BA, or TOP. This would include data that may be exchanged between a Responsible Entity's primary and backup Control Center.

Identification of Where Security Protection is Applied by the Responsible Entity

The SDT noted the need for a Responsible Entity to identify where it will apply protection for applicable data. The SDT did not specify the location where CIP-012-1 security protection must be applied. This allows latitude for Responsible Entities to implement the security controls in a manner best fitting their individual circumstances. This latitude ensures entities can still take advantage of security measures, such as deep packet inspection implemented at or near the EAP when ESPs are present, while maintaining the capability to protect the applicable data being transmitted between Control Centers.

The SDT also recognizes that CIP-012 security protection may be applied to a Cyber Asset that is not an identified BES Cyber Asset, Protected Cyber Asset, or EACMS. The identification of the Cyber Asset as the location where security protection is applied does not expand the scope of Cyber Assets identified as applicable under Cyber Security Standards CIP-002 through CIP-011.

The SDT understands that in data exchanges between Control Centers, a single entity may not be responsible for both ends of the communication link. The SDT intends for a Responsible Entity to identify only where it applied security protection. The Responsible Entity should not be held accountable for identifying where a neighboring entity applied security protection at the neighboring entity's facility. A Responsible Entity, however, may decide to take responsibility for both ends of a communication link. For example, it may place a router in a neighboring entity's data center. In a scenario where a Responsible Entity has taken responsibility for applying security protection on both ends of the communication link, the Responsible Entity should identify where it applied security protection at both ends of the link. The SDT intends for there to be alignment between the identification of where security protection is applied in CIP-012-1 Requirement R1, Part 1.2 and the identification of Responsible Entity responsibilities in CIP-012-1 Requirement R1, Part 1.3.

Control Center Ownership

The standard requirements address protection for Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers owned by a single Responsible Entity. They also cover the applicable data transmitted between Control Centers owned by two or more separate Responsible Entities. Unlike protection between a single Responsible Entity's Control Centers, applying protection between Control Centers owned by more than one Responsible Entity requires additional coordination. The requirements do not explicitly require formal agreements between Responsible Entities partnering for protection of applicable data. It is strongly recommended, however, that these partnering entities develop agreements, or use existing ones, to define responsibilities to ensure the security objective is met. An example noted in FERC Order No. 822 Paragraph 59 is, "if several registered entities have joint responsibility for a cryptographic key management system used between their respective Control Centers, they should have the prerogative to come to a consensus on which organization administers that particular key management system."

As an example, Figure 5 shows several data transmissions between Control Centers that a Responsible Entity should consider to be in-scope. The example does not include all possible scenarios. The solid green lines are in-scope communications and the dashed red lines are out-of-scope communications.

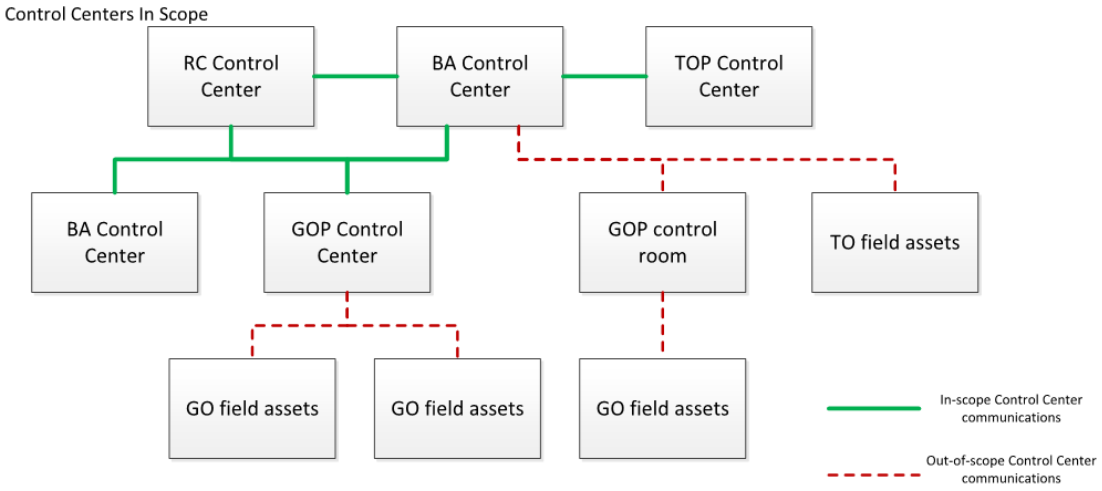


Figure 5: This reference model is an example and does not include all possible scenarios.

The SDT included Part 1.3 of the plan to address the situation when multiple registered entities are involved with protecting the data transmitted between Control Centers. Part 1.3 provides a mechanism to specify which entity is responsible for the application of security controls. The SDT included this requirement part to address security concerns as well as audit concerns. Where data is transmitted between different entities, the SDT asserts that it is necessary for both entities to understand the responsibilities of applying security controls to ensure the data is protected through its entire transmission and there is no security gap. The SDT also asserts this requirement part will provide evidence which may prevent the simultaneous auditing of multiple entities for each communication link between Control Centers when operated by different Responsible Entities. Security controls applied by the entity to achieve compliance with Parts 1.1 and 1.2 of the plan should correlate to the documented responsibilities in Part 1.3 of the entity's plan.

References

Here are several references to assist entities in developing plan(s) for protection of communication links:

- NIST Special Publication 800-53A, Revision 4: Security and Privacy Controls for Federal Information Systems and Organizations
- NIST Special Publication 800-82: Guide to Industrial Control Systems (ICS) Security
- NIST Special Publication 800-175B: Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms
- NIST Special Publication 800-47: Security Guide for Interconnecting Information Technology Systems

Exhibit G

Analysis of Violation Risk Factors and Violation Severity Levels

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Violation Risk Factor and Violation Severity Level Justifications

Project 2016-02 Modifications to CIP Standards

This document provides the standard drafting team's (SDT's) justification for assignment of violation risk factors (VRFs) and violation severity levels (VSLs) for each requirement in **CIP-012-1**. Each requirement is assigned a VRF and a VSL. These elements support the determination of an initial value range for the Base Penalty Amount regarding violations of requirements in FERC-approved Reliability Standards, as defined in the Electric Reliability Organizations (ERO) Sanction Guidelines. The SDT applied the following NERC criteria and FERC Guidelines when developing the VRFs and VSLs for the requirements.

NERC Criteria for Violation Risk Factors

High Risk Requirement

A requirement that, if violated, could directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures, or could hinder restoration to a normal condition.

Medium Risk Requirement

A requirement that, if violated, could directly affect the electrical state or the capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System. However, violation of a medium risk requirement is unlikely to lead to Bulk Electric System instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System. However, violation of a medium risk requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to Bulk Electric System instability, separation, or cascading failures, nor to hinder restoration to a normal condition.

Lower Risk Requirement
A requirement that is administrative in nature and a requirement that, if violated, would not be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System; or, a requirement that is administrative in nature and a requirement in a planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.

FERC Guidelines for Violation Risk Factors

Guideline (1) – Consistency with the Conclusions of the Final Blackout Report

FERC seeks to ensure that VRFs assigned to Requirements of Reliability Standards in these identified areas appropriately reflect their historical critical impact on the reliability of the Bulk-Power System. In the VSL Order, FERC listed critical areas (from the Final Blackout Report) where violations could severely affect the reliability of the Bulk-Power System:

- Emergency operations
- Vegetation management
- Operator personnel training
- Protection systems and their coordination
- Operating tools and backup facilities
- Reactive power and voltage control
- System modeling and data exchange
- Communication protocol and facilities
- Requirements to determine equipment ratings
- Synchronized data recorders
- Clearer criteria for operationally critical facilities
- Appropriate use of transmission loading relief.

Guideline (2) – Consistency within a Reliability Standard

FERC expects a rational connection between the sub-Requirement VRF assignments and the main Requirement VRF assignment.

Guideline (3) – Consistency among Reliability Standards

FERC expects the assignment of VRFs corresponding to Requirements that address similar reliability goals in different Reliability Standards would be treated comparably.

Guideline (4) – Consistency with NERC's Definition of the Violation Risk Factor Level

Guideline (4) was developed to evaluate whether the assignment of a particular VRF level conforms to NERC's definition of that risk level.

Guideline (5) – Treatment of Requirements that Co-mingle More Than One Obligation

Where a single Requirement co-mingles a higher risk reliability objective and a lesser risk reliability objective, the VRF assignment for such Requirements must not be watered down to reflect the lower risk level associated with the less important objective of the Reliability Standard.

NERC Criteria for Violation Severity Levels

VSLs define the degree to which compliance with a requirement was not achieved. Each requirement must have at least one VSL. While it is preferable to have four VSLs for each requirement, some requirements do not have multiple "degrees" of noncompliant performance and may have only one, two, or three VSLs.

VSLs should be based on NERC's overarching criteria shown in the table below:

Lower VSL	Moderate VSL	High VSL	Severe VSL
The performance or product measured almost meets the full intent of the requirement.	The performance or product measured meets the majority of the intent of the requirement.	The performance or product measured does not meet the majority of the intent of the requirement, but does meet some of the intent.	The performance or product measured does not substantively meet the intent of the requirement.

FERC Order of Violation Severity Levels

The FERC VSL guidelines are presented below, followed by an analysis of whether the VSLs proposed for each requirement in the standard meet the FERC Guidelines for assessing VSLs:

Guideline (1) – Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance

Compare the VSLs to any prior levels of non-compliance and avoid significant changes that may encourage a lower level of compliance than was required when levels of non-compliance were used.

Guideline (2) – Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties

A violation of a "binary" type requirement must be a "Severe" VSL.

Do not use ambiguous terms such as "minor" and "significant" to describe noncompliant performance.

Guideline (3) – Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement

VSLs should not expand on what is required in the requirement.

Guideline (4) – Violation Severity Level Assignment Should Be Based on a Single Violation, Not on a Cumulative Number of Violations

Unless otherwise stated in the requirement, each instance of non-compliance with a requirement is a separate violation. Section 4 of the Sanction Guidelines states that assessing penalties on a per violation per day basis is the "default" for penalty calculations.

VRF Justifications for CIP-012-1, Requirement R1	
Proposed VRF	**Medium**
NERC VRF Discussion	A VRF of Medium was assigned to this requirement. Cyber security plans enable effective implementation of the CIP standard's requirements to mitigate the risks posed by unauthorized disclosure and unauthorized modification of data used for Real-time Assessments and Real-time monitoring while being transmitted between Control Centers.
FERC VRF G1 Discussion Guideline 1- Consistency with Blackout Report	N/A
FERC VRF G2 Discussion Guideline 2- Consistency within a Reliability Standard	N/A
FERC VRF G3 Discussion Guideline 3- Consistency among Reliability Standards	The requirement complements CIP-005-1, Requirement R1, CIP-006-6, Requirement R1, and CIP-007-6, Requirement R1 which are related to security of networks and communications components. The proposed VRF is consistent with these related requirements.
FERC VRF G4 Discussion Guideline 4- Consistency with NERC Definitions of VRFs	Failure to have the required plan would not, under Emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.
FERC VRF G5 Discussion	N/A

VRF Justifications for CIP-012-1, Requirement R1	
Proposed VRF	**Medium**
Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation	

VSLs for CIP-012-1, Requirement R1			
Lower	**Moderate**	**High**	**Severe**
N/A	The Responsible Entity documented its plan(s) but failed to include one of the applicable Parts of the plan as specified in Requirement R1.	The Responsible Entity documented its plan(s) but failed to include two of the applicable Parts of the plan as specified in Requirement R1.	The Responsible Entity failed to document plan(s) for Requirement R1; Or The Responsible Entity failed to implement any Part of its plan(s) for Requirement R1, except under CIP Exceptional Circumstances.

VSL Justifications for CIP-012-1 Requirements R1	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The requirement is new. Therefore, the proposed VSL does not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The requirement is for the Responsible Entity to implement one or more documented plan(s) as specified in Requirement R1. The moderate VSL addresses where the Responsible Entity documented its plan(s) but failed to include one of the applicable parts of the plan as specified in Requirement R1. The high VSL addresses where the Responsible Entity documented its plan(s) but failed to include two of the applicable parts of the plan as specified in Requirement R1. The severe VSL addresses where the Responsible Entity failed to document plan(s) for Requirement R1, or where the Responsible Entity failed to implement plan(s) for Requirement R1.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL uses the same terminology as used in the associated requirement and is, therefore, consistent with the requirement.

FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Each VSL is based on a single violation and not cumulative violations.

Exhibit H

Summary of Development History and Complete Record of Development

Summary of Development History

Summary of Development History

The development record for proposed Reliability Standard CIP-012-1 is summarized below.

I. Overview of the Standard Drafting Team

When evaluating a proposed Reliability Standard, the Commission is expected to give "due weight" to the technical expertise of the ERO.[1] The technical expertise of the ERO is derived from the standard drafting team ("SDT") selected to lead each project in accordance with Section 4.3 of the NERC Standard Processes Manual.[2] For this project, the SDT consisted of industry experts, all with a diverse set of experiences. A roster of the Project 2016-02 – Modifications to CIP Standards SDT members is included in **Exhibit I**.

II. Standard Development History

A. Standard Authorization Request Development

Project 2016-02 – Modifications to CIP Standards was initiated on March 9, 2016 as a Standards Authorization Request ("SAR") to address Commission directives in Order No. 822 and other items.[3] The SAR was posted for a 30-day informal comment period from March 23, 2016 through April 21, 2016 and accepted by the Standards Committee on July 20, 2016. In Order No. 822, the Commission directed NERC to develop modifications to Reliability Standard CIP-006-6 to require Responsible Entities to implement controls to protect communication links and sensitive BES data communicated between BES Control Centers.[4] Rather than revise CIP-

---

1 Section 215(d)(2) of the Federal Power Act; 16 U.S.C. § 824(d)(2) (2012).

2 The NERC *Standard Processes Manual* is available at http://www.nerc.com/comm/SC/Documents/Appendix_3A_StandardsProcessesManual.pdf.

3 Order No. 822, *Revised Critical Infrastructure Protection Reliability Standards*, 154 FERC ¶ 61,037, *order denying reh'g*, Order No. 822-A, 156 FERC ¶ 61,037 (2016).

4 *Id*. at P 3.

006-6, the SDT determined that a new Reliability Standard was appropriate given the differences in applicability and scope between CIP-006-6 and proposed CIP-012-1.

B. First Posting - Comment Period, Initial Ballot and Non-binding Poll

Proposed Reliability Standard CIP-012-1, the associated Implementation Plan, Violation Risk Factors ("VRFs"), Violation Severity Levels ("VSLs"), and other associated documents were posted for a 45-day formal comment period from July 27, 2017 through September 11, 2017, with a parallel initial ballot and non-binding poll held during the last 10 days of the comment period from September 1, 2017 through September 11, 2017. The initial ballot for CIP-012-1 received 42.72 percent approval, reaching quorum at 80.26 percent of the ballot pool. The non-binding poll for the associated VRFs and VSLs received 41.53 percent supportive opinions, reaching quorum at 77.93 percent of the ballot pool. There were 81 sets of responses, including comments from approximately 207 different individuals and approximately 139 companies, representing all 10 industry segments.[5]

C. Second Posting - Comment Period, Additional Ballot and Non-binding Poll

Proposed Reliability Standard CIP-012-1, the associated Implementation Plan, VRFs, VSLs, and other associated documents were posted for a 45-day formal comment period from October 27, 2017 through December 11, 2017, with a parallel additional ballot as well as the non-binding poll held during the last 10 days of the comment period from December 1, 2017 through December 11, 2017 (the non-binding poll was extended from December 11, 2017 to December 12, 2017 to reach quorum). The additional ballot for CIP-012-1 reached quorum at 77.35 percent of the ballot pool and received 63.91 percent approval. The related non-binding

[5] NERC, *Consideration of Comments*, Project 2016-02 Modification to CIP Standards (CIP-012-1) (Oct. 2017), https://www.nerc.com/pa/Stand/Project%20201602%20Modifications%20to%20CIP%20Standards%20DL/2016-02_CIP-012-1_Consideration_of_Comments_10272017.pdf.

poll for CIP-012-1 reached quorum at 78.62 percent of the ballot pool and received 60.44 percent supportive opinions. There were 61 sets of responses, including comments from approximately 168 different individuals and approximately 117 companies, representing all 10 industry segments.[6]

D. Third Posting - Comment Period, Additional Ballot and Non-binding Poll

Proposed Reliability Standard CIP-012-1, the associated Implementation Plan, VRFs, VSLs, and other associated documents were posted for a 45-day formal comment period from March 16, 2018 through April 30, 2018, with a parallel additional ballot as well as the non-binding poll held during the last 10 days of the comment period from April 20, 2018 through April 30, 2018. The additional ballot for CIP-012-1 reached quorum at 78.32 percent of the ballot pool and received 83.71 percent approval. The related non-binding poll for CIP-012-1 reached quorum at 76.21 percent of the ballot pool and received 79.78 percent supportive opinions. There were 58 sets of responses, including comments from approximately 155 different individuals and approximately 108 companies, representing all 10 industry segments.[7]

E. Fourth Posting - Comment Period, Additional Ballot and Non-binding Poll

Proposed Reliability Standard CIP-012-1, the associated Implementation Plan, VRFs, VSLs, and other associated documents were posted for a 45-day formal comment period from May 18, 2018 through July 3, 2018, with a parallel additional ballot as well as the non-binding poll held during the last 10 days of the comment period from June 22, 2018 through July 3, 2018

---

[6] NERC, *Consideration of Comments*, Project 2016-02 Modification to CIP Standards (CIP-012-1) (Mar. 2018), https://www.nerc.com/pa/Stand/Project%20201602%20Modifications%20to%20CIP%20Standards%20DL/CIP-012-1_Consideration_of_Comments_03162018.pdf.

[7] NERC, *Consideration of Comments*, Project 2016-02 Modification to CIP Standards (CIP-012-1) (May 2018), https://www.nerc.com/pa/Stand/Project%20201602%20Modifications%20to%20CIP%20Standards%20DL/Project-2016-02_CIP-012-1_Consideration_of_Comments_Report_05252018.pdf.

(non-binding poll was extended an from July 3, 2018 to July 5, 2018 to reach quorum). The additional ballot for CIP-012-1 reached quorum at 75.4 percent of the ballot pool and received 68.45 percent approval. The related non-binding poll for CIP-012-1 reached quorum at 77.24 percent of the ballot pool and received 69.77 percent supportive opinions. There were 55 sets of responses, including comments from approximately 149 different individuals and approximately 101 companies, representing all 10 industry segments.[8]

F. Final Ballot

Proposed Reliability Standard CIP-012-1 was posted for a 10-day final ballot period from August 3, 2018 through August 13, 2018. The ballot for proposed Reliability Standard CIP-012-1 and associated documents reached quorum at 81.55 percent of the ballot pool, receiving support from 72.55 percent of the voters.

G. Board of Trustees Adoption

The NERC Board of Trustees adopted proposed Reliability Standard CIP-012-1 on August 16, 2018.[9]

---

[8] NERC, *Consideration of Comments*, Project 2016-02 Modification to CIP Standards (CIP-012-1) (Aug. 2018), https://www.nerc.com/pa/Stand/Project%20201602%20Modifications%20to%20CIP%20Standards%20DL/CIP-012-1_Consideration_of_Comments_08032018.pdf.

[9] NERC, *Board of Trustees Agenda Package*, Agenda Item 7da (CIP-012-1 – Cyber Security – Communications between Control Centers) *available at* https://www.nerc.com/gov/bot/Agenda%20highlights%20and%20Mintues%202013/Board_Open_Meeting_Agenda_Package_August_16_2018.pdf.

Complete Record of Development

Project 2016-02 Modifications to CIP Standards

Related Files

Status

A 45-day formal comment period for **CIP-002-6 - Cyber Security – BES Cyber System Categorization** and **CIP-003-8 - Cyber Security – Security Management Controls** is open through **8 p.m. Eastern, Tuesday, October 9, 2018**. Ballot pools are being formed through 8 **p.m. Eastern, Friday, September 21, 2018**. Initial ballots for the standards and non-binding polls of the associated Violation Risk Factors and Violation Severity Levels will be conducted **September 28 – October 9, 2018.**

The final ballot for **CIP-012-1 – Cyber Security - Communications between Control Centers** concluded **8 p.m. Eastern, Monday, August 13, 2018.** The voting results can be accessed via the link below. The standard will be submitted to the Board of Trustees for adoption and then filed with the appropriate regulatory authorities.

Background

The Version 5 Transition Advisory Group (V5 TAG) transferred issues to the Version 5 SDT that were identified during the industry transition to implementation of the Version 5 CIP Standards. Specifically, the issues that the SDT will address are:

- Cyber Asset and BES Cyber Asset Definitions
- Network and Externally Accessible Devices
- Transmission Owner (TO) Control Centers Performing Transmission Operator (TOP) Obligations
- Virtualization

On January 21, 2016, FERC issued Order No. 822 Revised Critical Infrastructure Protection Reliability Standards. In this order, FERC approved revisions to version 5 of the CIP standards and also directed that NERC address each of the Order 822 directives by developing modifications to requirements in CIP standards and the definition of Low Impact External Routable Connectivity (LERC), or the SDT shall develop an equally efficient and effective alternative. To address concerns identified in Order 822, the Commission directed the following:

- Develop modifications to the CIP Reliability Standards to provide mandatory protection for transient devices used at Low Impact BES Cyber Systems based on the risk posed to bulk electric system reliability.
- Develop modifications to the CIP Reliability Standards to require responsible entities to implement controls to protect, at a minimum, communication links and sensitive bulk electric system data communicated between bulk electric system Control Centers in a manner that is appropriately tailored to address the risks posed to the bulk electric system by the assets being protected (i.e., high, medium, or low impact).
- Develop a modification to provide the needed clarity, within one year of the effective date of this Final Rule, to the LERC definition consistent with the commentary in the Guidelines and Technical Basis section of CIP-003-6.

Standard(s) Affected – CIP-002-5.1, CIP-003-6, CIP-004-6, CIP-005-5, CIP-006-6, CIP-007-6, CIP-008-5, CIP-009-6, CIP-010-2, CIP-011-2, CIP-012-1

Purpose / Industry Need

The SDT will modify the CIP family of standards (or develop an equally efficient and effective alternative) to:

- Address issues identified by the CIP V5 TAG;
- Address FERC directives contained in Order 822; and
- Address requests for interpretations as directed by the NERC Standards

Draft	Actions	Dates	Results	Consideration of Comments
Final Draft CIP-012-1 Clean **(116)** | Redline to Last Posted **(117)** Implementation Plan **(118)** **Supporting Materials** VRF/VSL Justification Clean **(119)**| Redline to Last Posted **(120)** Technical Rationale Clean **(121)**| Redline to Last Posted **(122)** Implementation Guidance Clean **(123)** | Redline to Last Posted **(124)**	Final Ballot Info **(125)** Vote	08/03/18 - 08/13/18	Ballot Results **(126)**	
Draft 4 CIP-012-1 Clean **(96)** | Redline to Last Posted **(97)** Implementation Plan **(98)** **Supporting Materials** Unofficial Comment Form (Word) **(99)** VRF/VSL Justification Clean **(100)**| Redline to Last Posted **(101)** Technical Rationale Clean **(102)** | Redline to Last Posted **(103)** Implementation Guidance Clean **(104)**| Redline to Last Posted **(105)** Draft Reliability Standard Audit Worksheet (RSAW) Clean **(106)**| Redline to Draft 3 **(107)**	Comment Period Info **(108)** Submit Comments	05/18/18 - 07/03/18	Comments Received **(109)**	Consideration of Comments**(114)**
	Additional Ballot and Non-binding Poll Updated Info **(110)** Info **(111)** Vote	Additional Ballot 06/22/18 - 07/03/18 Non-binding Poll 6/22/18 - 7/5/18 Extended to reach quorum	Ballot Results **(112)** Non-binding Poll Results **(113)**	
	Info **(115)** Send RSAW feedback to: RSAWfeedback@nerc.net			

Standard Drafting Team Nominations **Supporting Materials** Unofficial Nomination Form (Word) **(94)**	Nomination Period Info **(95)** Submit Nominations	04/24/18 - 05/23/18		
Proposed Definition of Control Center **(84)** Implementation Plan **(85)** **Supporting Materials** Unofficial Comment Form (Word) **(86)**	Initial Ballots for the Definition and Implementation Plan Updated Info **(87)** Info **(88)** Vote	04/20/18 - 04/30/18	Definition Ballot Results **(89)** Implementation Plan Ballot Results **(90)**	
	Comment Period Info **(91)** Submit Comments	03/16/18 - 04/30/18	Comments Received **(92)**	Consideration of Comments **(93)**
	Join Ballot Pools	03/16/18 - 04/16/18		
Draft 3 CIP-012-1 Clean **(63)** | Redline to Last Posted **(64)** Implementation Plan **(65)** **Supporting Materials** Unofficial Comment Form (Word) **(66)** Consideration of Issues and Directives Clean **(67)** | Redline to Last Posted **(68)**	Additional Ballot and Non-binding Poll Updated Info **(77)** Info **(78)** Vote	04/20/18 - 04/30/18	Ballot Results **(79)** Non-binding Poll Results **(80)**	

VRF/VSL Justification Clean **(69)** | Redline to Last Posted **(70)** Implementation Guidance Clean **(71)** | Redline to Last Posted **(72)** Technical Rationale Clean **(73)** | Redline to Last Posted **(74)** Draft Reliability Standard Audit Worksheet (RSAW) Clean **(75)** | Redline to Draft 2 **(76)**	Comment Period Info **(81)** Submit Comments	03/16/18 - 04/30/18	Comments Received **(82)**	Consideration of Comments **(83)**
	Send RSAW feedback to: RSAWfeedback@nerc.net			
Technical Rationale and Justification for CIP-012-1 **(57)** Implementation Guidance for CIP-012-1 **(58)** **Supporting Materials** Unofficial Comment Form (Word) **(59)**	Comment Period Info **(60)** Submit Comments	11/20/17 - 12/11/17	Comments Received **(61)**	Consideration of Comments **(62)**
Draft 2 CIP-012-1 Clean **(38)** | Redline to Last Posted **(39)** Implementation Plan Clean **(40)** | Redline to Last Posted **(41)** **Supporting Materials** Unofficial Comment Form (Word) **(42)** Consideration of Issues and Directives	Additional Ballot and Non-binding Poll Updated Info **(49)** Info **(50)** Vote	12/01/17 - 12/11/17 (The Non-binding Poll was extended to 12/12/17 to reach quorum)	Ballot Results **(51)** Non-Binding Poll Results **(52)**	
	Comment Period Info **(53)** Submit Comments	10/27/17 - 12/11/17	Comments Received **(54)**	Consideration of Comments **(56)**

Clean **(43)** | Redline to Last Posted **(44)** VRF/VSL Justification Clean **(45)** | Redline to Last Posted **(46)** Draft Reliability Standard Audit Worksheet (RSAW) Clean **(47)** | Redline to Last Posted **(48)**	Info **(55)** Send RSAW feedback to: RSAWfeedback@nerc.net	12/01/17 - 12/11/17		
Proposed Definition of Control Center **(31)** Technical Rationale and Justification for CIP-012-1 **(32)** **Supporting Materials** Unofficial Comment Form - Proposed Definition of Control Center **(33)** Unofficial Comment Form - Technical Rationale and Justification for CIP-012-1 **(34)**	Comment Periods Info**(35)** Submit Comments	08/14/17 - 09/12/17	Comments Received Proposed Definition of Control Center **(36)** Technical Rationale and Justification for CIP-012-1 **(37)**	
Draft 1 CIP-012-1 **(17)** Implementation Plan **(18)** **Supporting Materials** Unofficial Comment Form (Word) **(19)** Consideration of Issues and Directives **(20)** VRF/VSL Justification **(21)**	Initial Ballot and Non-binding Poll Updated Info **(23)** Info **(24)** Vote	09/01/17 - 09/11/17	Ballot Results **(25)** Non-binding Poll Results **(26)**	
	Comment Period Info **(27)** Submit Comments	07/27/17 - 09/11/17	Comments Received **(28)**	Consideration of Comments **(29)**
	Join Ballot Pools	07/27/17 - 08/25/17		
	Info **(30)**			

Draft Reliability Standard Audit Worksheet (RSAW) **(22)**	Send RSAW feedback to: RSAWfeedback@nerc.net	08/17/17 - 09/11/17		
Communication Networks/Unofficial Comment Form (14)	Comment Period Info **(15)** Submit Comments	02/10/17 - 03/13/17	Comments Received **(16)**	
The Standards Committee accepted the Standards Authorization Request on July 20, 2016				
Standards Authorization Request Clean **(8)** | Redline to Last Posted **(9)** **Supporting Materials** Unofficial Comment Form **(10)** CIP Version 5 Transition Advisory Group Issues for Consideration **(11)**	Comment Period Info **(12)** Submit Comments	06/01/16 - 06/30/16	Comments Received **(13)**	
Standards Authorization Request **(3)** **Supporting Materials** Unofficial Comment Form (Word) **(4)** CIP Version 5 Transition Advisory Group Issues for Consideration **(5)**	Comment Period Info **(6)** Submit Comments	03/23/16 - 04/21/16	Comments Received **(7)**	
Supplemental Standard Drafting Team Nominations **Supporting Materials** Unofficial Nomination Form (Word) **(1)**	Nomination Period Info **(2)** Submit Nominations	03/10/16 - 03/23/16		

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Nomination Form

Project 2016-02 Modifications to CIP Standards

Supplemental Nomination Period

Nominations for additional standard drafting team (SDT) members are being solicited for **Project 2016-02 Modifications to CIP Standards**. Use the electronic form to submit nominations by **8 p.m. Eastern, Wednesday, March 23, 2016.** This unofficial version is provided to assist nominees in compiling the information necessary to submit the electronic form.

Documents and information about this project are available on the Project 2016-02 Modifications to CIP Standards page. If you have questions, contact either Senior Standards Developer, Stephen Crutchfield at (609) 651-9455 or Al McMeekin at (404) 446-9675.

By submitting a nomination form, you are indicating your willingness and agreement to actively participate in face-to-face meetings and conference calls.

Previous drafting or review team experience is beneficial, but not required. A brief description of the desired qualifications, expected commitment, and other pertinent information is included below.

Background

This solicitation for nominations is to supplement the existing Project 2016-02 Modifications to CIP Standards SDT that is continuing to address the work in the Project 2016-02 Modifications to CIP Standards Authorization Request (SAR). NERC is seeking individuals from the United States and Canada who possess experience in one or more of the following areas:

- Operations technology
- Communication networks
- Virtualization
- Protection of transient electronic devices
- Network and externally accessible devices
- Cyber Asset and BES Cyber Asset definitions
- Transmission Owner (TO) Control Centers
- Critical Infrastructure Protection ("CIP") family of Reliability Standards

The time commitment for Project 2016-02 is expected to be significant. Participants should anticipate an average workload of 20 hours per week devoted to the drafting team efforts. In-person meetings will occur typically for 2 ½ - 3 days most months (not including travel time) and meetings will take place in different parts of North America. When not meeting in person, regularly scheduled

conference calls will be used to conduct drafting team work. Outside the scheduled meetings, individuals or subgroups will have additional preparation and support work such as researching and developing proposed concepts, reviewing proposals, compiling comments and drafting responses, etc. Lastly, outreach is an important component of this drafting team's effort. Members of the team are expected to interact with other stakeholders during the revision development process.

Name:	
Organization:	
Address:	
Telephone:	
E-mail:	

Please briefly describe your experience and qualifications to serve on the requested Standard Drafting Team (Bio):

If you are currently a member of any NERC drafting team, please list each team here:

☐ Not currently on any active SAR or standard drafting team.

☐ Currently a member of the following SAR or standard drafting team(s):

If you previously worked on any NERC drafting team please identify the team(s):

☐ No prior NERC SAR or standard drafting team.

☐ Prior experience on the following team(s):

Select each NERC Region in which you have experience relevant to the Project for which you are volunteering:

☐ FRCC	☐ RF	☐ Texas RE
☐ MRO	☐ SERC	☐ WECC
☐ NPCC	☐ SPP RE	☐ NA – Not Applicable

Select each Industry Segment that you represent:

☐	1 — Transmission Owners

☐	2 — RTOs, ISOs
☐	3 — Load-serving Entities
☐	4 — Transmission-dependent Utilities
☐	5 — Electric Generators
☐	6 — Electricity Brokers, Aggregators, and Marketers
☐	7 — Large Electricity End Users
☐	8 — Small Electricity End Users
☐	9 — Federal, State, and Provincial Regulatory or other Government Entities
☐	10 — Regional Reliability Organizations and Regional Entities
☐	NA – Not Applicable

Select each Function[1] in which you have current or prior expertise:

☐ Balancing Authority	☐ Transmission Operator
☐ Compliance Enforcement Authority	☐ Transmission Owner
☐ Distribution Provider	☐ Transmission Planner
☐ Generator Operator	☐ Transmission Service Provider
☐ Generator Owner	☐ Purchasing-selling Entity
☐ Interchange Authority	☐ Reliability Coordinator
☐ Load-serving Entity	☐ Reliability Assurer
☐ Market Operator	☐ Resource Planner
☐ Planning Coordinator	

Provide the names and contact information for two references who could attest to your technical qualifications and your ability to work well in a group:

Name:		Telephone:	
Organization:		E-mail:	
Name:		Telephone:	
Organization:		E-mail:	

[1] These functions are defined in the NERC Functional Model, which is available on the NERC web site.

Provide the name and contact information of your immediate supervisor or a member of your management who can confirm your organization's willingness to support your active participation.			
Name:		Telephone:	
Title:		Email:	

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2016-02 Modifications to CIP Standards

Supplemental Nomination Period Open through March 23, 2016

Now Available

Nominations are being sought for additional standard drafting team (SDT) members through **8 p.m. Eastern, Wednesday, March 23, 2016**.

Use the electronic form to submit a nomination. If you experience any difficulties in using the electronic form, contact Wendy Muller. An unofficial Word version of the nomination form is posted on the Standard Drafting Team Vacancies page and the project page.

By submitting a nomination form, you are indicating your willingness and agreement to actively participate in face-to-face meetings and conference calls.

Previous drafting or review team experience is beneficial, but not required.

The time commitment for this project is expected to be significant. Participants should anticipate an average workload of 20 hours per week devoted to the SDT efforts. In person meetings will occur typically for 2 ½ - 3 days most months (not including travel time) and meetings will take place in different parts of North America. When not meeting in person, regularly scheduled conference calls will be used to conduct drafting team work. Outside the scheduled meetings, individuals or subgroups will have additional preparation and support work such as researching and developing proposed concepts, reviewing proposals, compiling comments and drafting responses, etc. Lastly, outreach is an important component of this SDT's effort. Members of the team are expected to interact with other stakeholders during the revision development process.

See the project page and unofficial nomination form for more information.

Next Steps

The Standards Committee is expected to appoint members to the team in April 2016. Nominees will be notified shortly after they have been appointed.

For information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact either Senior Standards Developer, Stephen Crutchfield at (609) 651-9455 or Al McMeekin at (404) 446-9675.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326

404-446-2560 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Authorization Request Form

When completed, email this form to:
sarcomm@nerc.com

NERC welcomes suggestions to improve the reliability of the bulk power system through improved reliability standards. Please use this form to submit your request to propose a new or a revision to a NERC's Reliability Standard.

Request to propose a new or a revision to a Reliability Standard			
Title of Proposed Standard(s):	Modifications to CIP Standards		
Date Submitted:	March 9, 2016		
SAR Requester Information			
Name:	Stephen Crutchfield		
Organization:	NERC		
Telephone:	609-651-9455	E-mail:	Stephen.Crutchfield@nerc.net
SAR Type (Check as many as applicable)			
☒ New Standard		☒ Withdrawal of existing Standard	
☒ Revision to existing Standard		☐ Urgent Action	

SAR Information
Purpose (Describe what the standard action will achieve in support of Bulk Electric System reliability.):
The purpose of this project is to (1) consider the Version 5 Transition Advisory Group (V5TAG) issues identified in the *CIP V5 Issues for Standard Drafting Team Consideration* (V5TAG Transfer Document) and (2) address the Federal Energy Regulatory Commission (Commission) directives contained in Order 822. These revisions will increase reliability and security to the Bulk-Power System (BPS) by enhancing cyber protection of BPS facilities.
Industry Need (What is the industry problem this request is trying to solve?):
The V5TAG, which consists of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP version 5 standards and to support industry's implementation activities. During the course of the V5TAG's activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by the existing standard drafting team (SDT) for the CIP Reliability Standards.

SAR Information

The V5 TAG developed the V5TAG Transfer Document to explain the issues and recommend that the SDT consider them in future development activity.

On January 21, 2016, the Commission issued Order No. 822 approving revisions to the CIP version 5 standards and also directing NERC to develop modifications to address:

- Protection of transient electronic devices used at low-impact BES Cyber Systems;
- Protections for communication network components between control centers; and
- Refinement of the Low Impact External Routable Connectivity (LERC) definition.

The Commission did not provide a date by which the modifications for transient devices or communication networks must be completed. For the LERC definition, however, the Commission directed that NERC submit the modification within one year of the effective date of Order No. 822 (March 31, 2017).

Brief Description (Provide a paragraph that describes the scope of this standard action.)

The proposed project will consider the issues raised by the V5TAG in the V5TAG Transfer Document and will address the Commission directives in Order No. 822 through modifications to the CIP standards. The work will include development of Violation Risk Factors, Violation Severity Levels, and an Implementation Plan for the modified standards and will meet the deadlines established by the Commission in Order No. 822.

Detailed Description (Provide a description of the proposed project with sufficient details for the standard drafting team to execute the SAR. Also provide a justification for the development or revision of the standard, including an assessment of the reliability and market interface impacts of implementing or not implementing the standard action.)

As stated above, the purpose of this project is to consider the V5TAG issues in the initial transfer document V5TAG Transfer Document and address the Commission directives contained in Order 822. For the directive on the LERC definition, the project is to respond within the deadline required in the order.

As noted above, the V5TAG identified specific issues with the CIP V5 standards. The V5TAG drafted the V5TAG Transfer Document to formally recommend that the SDT address these issues during standards development to consider whether modifications can be made to the standard language. As outlined in the V5TAG Transfer Document, the specific issues are as follows:

- 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. The V5TAG recommends the following enhancements:
    - Clarify the intent of “programmable” in Cyber Asset.
    - Clarify and focus the definition of “BES Cyber Asset” including:

SAR Information

- 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.

- 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"
  - The meaning of the word 'associated' in the ERC definition.
  - The applicability of ERC including the concept of the term "directly" used in the phrase "cannot be directly accessed through External Routable Connectivity" within the Applicability section.
  - The IRA definition placement of the phrase "using a routable protocol" in the definition and with respect to Dial-up Connectivity.
  - The Guidelines and Technical Basis sentence, "If dial-up connectivity is used for Interactive Remote Access, then Requirement R2 also applies."
- Transmission Owner (TO) Control Centers Performing Transmission Operator (TOP) Obligations – V5TAG is aware of multiple interpretations of the language "used to perform the functional obligation of" in CIP-002-5.1 Attachment 1, section 2.12 and recommends clarification of:
  - The applicability of requirements on a TO Control Center that performs the functional obligations of a TOP, particularly if the TO has the ability to operate switches, breakers and relays in the BES.
  - The definition of Control Center.
  - The language scope of "perform the functional obligations of" throughout the Attachment 1 criteria.
- Virtualization – The CIP V5 standards do not specifically address virtualization. Because of the increasing use of virtualization in industrial control system environments, 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.

The SDT shall also address the Order No. 822 directives by developing modifications to requirements in CIP standards and the definition of LERC. The Commission directed the following:

- *Per paragraph 32, "...we direct that NERC, pursuant to section 215(d)(5) of the FPA, develop modifications to the CIP Reliability Standards to provide mandatory protection for transient devices used at Low Impact BES Cyber Systems based on the risk posed to bulk electric system reliability. While NERC has flexibility in the manner in which it addresses the Commission's concerns, the proposed modifications should be designed to effectively address the risks posed by*

SAR Information
transient devices to Low Impact BES Cyber Systems in a manner that is consistent with the risk-based approach reflected in the CIP version 5 Standards." • *Per paragraph 53, "…the Commission concludes that modifications to CIP-006-6 to provide controls to protect, at a minimum, communication links and data communicated between bulk electric system Control Centers are necessary in light of the critical role Control Center communications play in maintaining bulk electric system reliability. Therefore, we adopt the NOPR proposal and direct that NERC, pursuant to section 215(d)(5) of the FPA, develop modifications to the CIP Reliability Standards to require responsible entities to implement controls to protect, at a minimum, communication links and sensitive bulk electric system data communicated between bulk electric system Control Centers in a manner that is appropriately tailored to address the risks posed to the bulk electric system by the assets being protected (i.e., high, medium, or low impact)."* • *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 to provide the needed clarity, within one year of the effective date of this Final Rule…."*

Reliability Functions	
The Standard will Apply to the Following Functions (Check each one that applies.)	
☐ Regional Reliability Organization	Conducts the regional activities related to planning and operations, and coordinates activities of Responsible Entities to secure the reliability of the Bulk Electric System within the region and adjacent regions.
☒ Reliability Coordinator	Responsible for the real-time operating reliability of its Reliability Coordinator Area in coordination with its neighboring Reliability Coordinator's wide area view.
☒ Balancing Authority	Integrates resource plans ahead of time, and maintains load-interchange-resource balance within a Balancing Authority Area and supports Interconnection frequency in real time.

Reliability Functions		
☒	Interchange Authority	Ensures communication of interchange transactions for reliability evaluation purposes and coordinates implementation of valid and balanced interchange schedules between Balancing Authority Areas.
☐	Planning Coordinator	Assesses the longer-term reliability of its Planning Coordinator Area.
☐	Resource Planner	Develops a >one year plan for the resource adequacy of its specific loads within a Planning Coordinator area.
☐	Transmission Planner	Develops a >one year plan for the reliability of the interconnected Bulk Electric System within its portion of the Planning Coordinator area.
☒	Transmission Service Provider	Administers the transmission tariff and provides transmission services under applicable transmission service agreements (e.g., the pro forma tariff).
☒	Transmission Owner	Owns and maintains transmission facilities.
☒	Transmission Operator	Ensures the real-time operating reliability of the transmission assets within a Transmission Operator Area.
☐	Distribution Provider	Delivers electrical energy to the End-use customer.
☒	Generator Owner	Owns and maintains generation facilities.
☒	Generator Operator	Operates generation unit(s) to provide real and Reactive Power.
☐	Purchasing-Selling Entity	Purchases or sells energy, capacity, and necessary reliability-related services as required.
☐	Market Operator	Interface point for reliability functions with commercial functions.
☐	Load-Serving Entity	Secures energy and transmission service (and reliability-related services) to serve the End-use Customer.

Reliability and Market Interface Principles	
Applicable Reliability Principles (Check all that apply).	
☐	1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.
☐	2. The frequency and voltage of interconnected bulk power systems shall be controlled within defined limits through the balancing of real and Reactive Power supply and demand.

Reliability and Market Interface Principles	
☐	3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.
☐	4. Plans for emergency operation and system restoration of interconnected bulk power systems shall be developed, coordinated, maintained and implemented.
☒	5. Facilities for communication, monitoring and control shall be provided, used and maintained for the reliability of interconnected bulk power systems.
☐	6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions.
☐	7. The security of the interconnected bulk power systems shall be assessed, monitored and maintained on a wide area basis.
☒	8. Bulk power systems shall be protected from malicious physical or cyber attacks.

Does the proposed Standard comply with all of the following Market Interface Principles?	Enter (yes/no)
1. A reliability standard shall not give any market participant an unfair competitive advantage.	YES
2. A reliability standard shall neither mandate nor prohibit any specific market structure.	YES
3. A reliability standard shall not preclude market solutions to achieving compliance with that standard.	YES
4. A reliability standard shall not require the public disclosure of commercially sensitive information. All market participants shall have equal opportunity to access commercially non-sensitive information that is required for compliance with reliability standards.	YES

Related Standards	
Standard No.	Explanation

Related SARs	
SAR ID	Explanation

Regional Variances	
Region	Explanation
FRCC	
MRO	
NPCC	
RF	
SERC	
SPP RE	
Texas RE	
WECC	

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Comment Form

Project 2016-02 Modifications to CIP Standards Standards Authorization Request (SAR)

Do not use this form for submitting comments. Use the electronic form to submit comments on the Project 2016-02 Modifications to CIP Standards SAR. The electronic comment form must be submitted by **8 p.m. Eastern, Thursday, April 21, 2016**.

Documents and information about this project are available on the Project 2016-02 Modifications to CIP Standards. If you have questions, contact either Senior Standards Developer, Stephen Crutchfield at (609) 651-9455 or Al McMeekin at (404) 446-9675.

Background Information

On January 21, 2016, FERC issued Order No. 822, *Revised Critical Infrastructure Protection Reliability Standards,* approving seven CIP Reliability Standards and new or modified definitions. FERC also directed NERC to develop modifications to address:

- Protection of transient electronic devices used at low-impact bulk electric system cyber systems;
- Protections for communication network components between control centers; and
- Refinement of the definition for Low Impact External Routable Connectivity (LERC)

FERC directed NERC to submit new or modified standards responding to the directives related to the definition of LERC by March 30, 2016, one year from the effective date of Order No. 822. FERC did not place any time frame for NERC to respond to the remaining directives.

The CIP Version 5 Transition Advisory Group (V5 TAG) transferred issues to the CIP Version 5 Standard Drafting Team (SDT) that were identified during the industry transition to implementation of the CIP Version 5 Standards. Specifically, the issues that the SDT will address are:

- Cyber Asset and BES Cyber Asset Definitions
- Network and Externally Accessible Devices
- Transmission Owner Control Centers Performing Transmission Operator Obligations
- Virtualization

On March 9, 2016, the NERC Standards Committee accepted and authorized the posting of the Modifications to CIP Standards SAR. It is posted for a 30-day informal comment period because it is addressing FERC directives.

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:

   Comments:

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:

   Comments:

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

   Yes:

   No:

   Comments:

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP V5 Issues for Standard Drafting Team Consideration

September 15, 2015

From experience in the V5 Transition Study and the on-going implementation efforts, the CIP Version 5 Transition Advisory Group (V5TAG) identified specific issues with the CIP Version 5 standard language that caused difficulty in implementation of the requirements. In many cases, the V5TAG members found that select language within the CIP Version 5 standards may be understood in multiple ways. These interpretations appear to go beyond the intended flexibility of the standard language that is necessary to accommodate the diverse nature of facts and circumstances across the electric sector. At this time, the V5TAG proposes the following issues to be addressed by the CIP V5 Revisions drafting team (SDT) or other appropriate team for standards development:

- **Cyber Asset and BES Cyber Asset definitions**

  The foundational definition for the CIP Version 5 standards is 'Cyber Assets.' When Cyber Assets meet a threshold of Bulk Electric System (BES) impact they become 'BES Cyber Assets (BCA)' which are grouped, by a Responsible Entity, into 'BES Cyber Systems (BCS).' Viewing BCAs too broadly can lead to many thousands of devices in the typical utility becoming an administrative burden for which few if any cyber security controls can actually be applied or where there is limited associated cyber security risk. Vast amounts of effort would be expended for these types of cyber assets to track and document their lack of capability for even the most basic cyber security controls. Viewing BCAs too narrowly could lead to missing consideration of devices that have a sufficient level of cyber capability and risk impact.

  The SDT should consider the definition of Cyber Asset and clarify the intent of "programmable" by considering such factors as if a device is merely configurable, its executable code is not field upgradable, or if its functionality can only be changed via physical DIP switches, swapping internal chips, etc.

  The SDT should consider clarifying and focusing the definition of "BES Cyber Asset" including:

  a. Focusing the definition so that it does not subsume all other cyber asset types. Protected Cyber Assets (PCA), by nature of being on the same network, can have some form of adverse impact if misused. Electronic Access Control or Monitoring Systems (EACMS) if misused or unavailable can have some form of adverse impact. This can result in a "hall of

mirrors" effect where everything in or that creates an Electronic Security Perimeter (ESP) also meets the BCA definition.

b. Considering if there is a lower bound to the term 'adverse' in "adverse impact". For example, is the focus of a typical generating unit the servers and operator human machine interfaces (HMI) and controller cabinets and Programmable Logic Controllers (PLCs) or is it the thousands of individual sensors and transmitters throughout the plant?

c. Clarify 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.

- **Network and Externally Accessible Devices (ERC, ESP, IRA)**

  The SDT should consider the concepts and requirements concerning Electronic Security Perimeters (ESP), External Routable Connectivity (ERC), and Interactive Remote Access (IRA) including:

  a. Clarify 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.

  b. The word 'associated' in the ERC definition is unclear in that it alludes to some form of relationship but does not define the relationship between the items. Striking 'associated' and defining the intended relationship would provide much needed clarity.

  c. Review of the applicability of ERC including the concept of the term "directly" used in the phrase "cannot be directly accessed through External Routable Connectivity" within the Applicability section. As well, consider the interplay between IRA and ERC.

  d. Clarify the IRA definition to address the placement of the phrase "using a routable protocol" in the definition and clarity with respect to Dial-up Connectivity.

  e. Address the Guidelines and Technical Basis sentence, "If dial-up connectivity is used for Interactive Remote Access, then Requirement R2 also applies."

- **Transmission Owner (TO) Control Centers Performing Transmission Operator (TOP) Obligations**

  CIP-002-5.1 Attachment 1 – Impact Reliability Criteria, sections 1.1, 1.2, 1.3, 1.4, 2.11, 2.12, and 2.13 employ the language "used to perform the functional obligation of", and then lists the functional registration. It was intended that this caveat would capture entities that perform obligations of a specific registered function, whether they are registered for that function or not. However, this language has caused confusion, especially in section 2.12 concerning TOP Control Centers. The term "functional obligation" may be interpreted to have different meaning in a variety of situations.

One interpretation is for the defined term Control Center to be strictly associated with the Balancing Authority (BA), Generator Operator (GOP), Reliability Coordinator (RC), and Transmission Operator (TOP) functional registrations, and that control rooms or dispatch centers owned and operated by Transmission Owners (TOs) with control of limited BES facilities would be excluded. A second interpretation may expand or contract the applicability of the Control Center designation, based on criteria that may not take into consideration overall risk to reliable operations of the BES.

Early analysis found the potential for TOs (not Registered as TOPs) that only operate limited breakers to be pulled in as medium impact Control Centers, even if the few Facilities they control are low impact. (For example, an entity with one 161kV breaker in one substation and a second 161kV breaker in a different substation, both breakers associated with low impact Facilities.) As currently written, low impact Control Centers are to be identified per criteria 3.1 and could be commensurate with risk for these scenarios.

Areas for the SDT to address are:

a. CIP-002-5.1, Attachment 1 Control Center criteria for additional clarity and for possible revisions related to TOP or TO Control Centers performing the functional obligations of a TOP, in particular for small or lower-risk entities. A potential revision could be a size for criteria 2.12, Control Centers performing the functional obligations of a TOP.
b. Clarify the applicability of requirements on a TO Control Center that perform the functional obligations of a TOP, particularly if the TO has the ability to operate switches, breakers and relays in the BES. Review the corresponding Guidelines and Technical Basis of CIP-002-5.1, specifically: the "CIP-002-5" section paragraph starting with "Responsibility for the reliable operation of the BES is spread across all Entity Registrations"; the table following that paragraph; the "High Impact Rating (H)" section; and the criterion bullets for Control Centers under the "Medium Impact Rating (M)" section.
c. The definition of Control Center (if pursued, recognize possible impacts on operations and planning standards and/or glossary terms that include 'Control Center', for example, the revised Glossary term for "System Operator" to be effective July 1, 2016).
d. The language scope of "perform the functional obligations of" throughout the Attachment 1 criteria.

- **<u>Virtualization</u>**

  The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration.

The SDT should consider revisions to CIP-005 and the definitions of Cyber Asset and Electronic Access Point that make clear the permitted architecture and address the security risks of network, server and storage virtualization technologies.

The transition to CIP Version 5 continues as the compliance deadline of April 1, 2016 approaches. The V5TAG continues to discuss challenging issues being undertaken during the on-going implementation. The group may find additional issues to transfer to the SDT for consideration.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2016-02 Modifications to CIP Standards Standards Authorization Request

Informal Comment Period Open through April 21, 2016

Now Available

A 30-day informal comment period for the **Project 2016-02** Standard Authorization Request (SAR), is open through **8 p.m. Eastern, Thursday, April 21, 2016**.

Commenting

Use the electronic form to submit comments on the SAR. If you experience any difficulties in using the electronic form, contact Wendy Muller. An unofficial Word version of the comment form is posted on the project page.

If you are having difficulty accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out, contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 8 p.m. Eastern).

Next Steps

The drafting team will consider all responses received during the comment period and determine the next steps of the project

For more information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact either Senior Standards Developer, Stephen Crutchfield at (609) 651-9455 or Al McMeekin at (404) 446-9675.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

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:

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Authorization Request Form

When completed, email this form to:
sarcomm@nerc.com

NERC welcomes suggestions to improve the reliability of the bulk power system through improved reliability standards. Please use this form to submit your request to propose a new or a revision to a NERC's Reliability Standard.

Request to propose a new or a revision to a Reliability Standard			
Title of Proposed Standard(s):	Modifications to CIP Standards		
Date Submitted:	June 1, 2016		
SAR Requester Information			
Name:	Stephen Crutchfield		
Organization:	NERC		
Telephone:	609-651-9455	E-mail:	Stephen.Crutchfield@nerc.net
SAR Type (Check as many as applicable)			
☒ New Standard		☒ Withdrawal of existing Standard	
☒ Revision to existing Standard		☐ Urgent Action	

SAR Information
Purpose (Describe what the standard action will achieve in support of Bulk Electric System reliability.):
The purpose of this project is to (1) consider the Version 5 Transition Advisory Group (V5TAG) issues identified in the *CIP V5 Issues for Standard Drafting Team Consideration* (V5TAG Transfer Document) and (2) address the Federal Energy Regulatory Commission (Commission) directives contained in Order 822. These revisions will increase reliability and security to the Bulk-Power System (BPS) by enhancing cyber protection of BPS facilities.
Industry Need (What is the industry problem this request is trying to solve?):
The V5TAG, which consists of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP V5 standards and to support industry's implementation activities. During the course of the V5TAG's activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by the existing standard drafting team (SDT) for the CIP Reliability Standards.

SAR Information

The V5TAG developed the V5TAG Transfer Document to explain the issues and recommend that the SDT consider them in future development activity.

On January 21, 2016, the Commission issued Order No. 822 approving revisions to the CIP version 5 standards and also directing NERC to develop modifications to address:

- Protection of transient electronic devices used at low-impact BES Cyber Systems;
- Protections for communication network components between control centers; and
- Refinement of the Low Impact External Routable Connectivity (LERC) definition.

The Commission did not provide a date by which the modifications for transient devices or communication networks must be completed. For the LERC definition, however, the Commission directed that NERC submit the modification within one year of the effective date of Order No. 822 (March 31, 2017).

Brief Description (Provide a paragraph that describes the scope of this standard action.)

The proposed project will consider the issues raised by the V5TAG in the V5TAG Transfer Document and will address the Commission directives in Order No. 822 through modifications to the CIP standards. The work will include development of Violation Risk Factors, Violation Severity Levels, and an Implementation Plan for the modified standards and will meet the deadlines established by the Commission in Order No. 822.

Detailed Description (Provide a description of the proposed project with sufficient details for the standard drafting team to execute the SAR. Also provide a justification for the development or revision of the standard, including an assessment of the reliability and market interface impacts of implementing or not implementing the standard action.)

As stated above, the purpose of this project is to consider the V5TAG issues in the initial transfer document V5TAG Transfer Document and address the Commission directives contained in Order 822. For the directive on the LERC definition, the project is to respond within the deadline required in the order.

As noted above, the V5TAG identified specific issues with the CIP V5 standards. The V5TAG drafted the V5TAG Transfer Document to formally recommend that the SDT address these issues during standards development to consider whether modifications can be made to the standard language. As outlined in the V5TAG Transfer Document, the specific issues are as follows:

- 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. 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”.

SAR Information

- 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.

- 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"
  - The meaning of the word 'associated' in the ERC definition.
  - The applicability of ERC including the concept of the term "directly" used in the phrase "cannot be directly accessed through External Routable Connectivity" within the Applicability section.
  - The IRA definition placement of the phrase "using a routable protocol" in the definition and with respect to Dial-up Connectivity.
  - The Guidelines and Technical Basis sentence, "If dial-up connectivity is used for Interactive Remote Access, then Requirement R2 also applies."
- Transmission Owner (TO) Control Centers Performing Transmission Operator (TOP) Obligations – V5TAG is aware of multiple interpretations of the language "used to perform the functional obligation of" in CIP-002-5.1 Attachment 1, section 2.12 and recommends clarification of:
  - The applicability of requirements on a TO Control Center that performs the functional obligations of a TOP, particularly if the TO has the ability to operate switches, breakers and relays in the BES.
  - The definition of Control Center.
  - The language scope of "perform the functional obligations of" throughout the Attachment 1 criteria.
- Virtualization – The CIP V5 standards do not specifically address virtualization. Because of the increasing use of virtualization in industrial control system environments, V5TAG asked that the SDT consider the CIP V5 standards and the associated definitions regarding permitted architecture and the security risks of virtualization technologies.

The SDT shall also address the Order No. 822 directives by developing modifications to requirements in CIP standards and the definition of LERC. The Commission directed the following:

- *Per paragraph 32, "...we direct that NERC, pursuant to section 215(d)(5) of the FPA, develop modifications to the CIP Reliability Standards to provide mandatory protection for transient devices used at Low Impact BES Cyber Systems based on the risk posed to bulk electric system reliability. While NERC has flexibility in the manner in which it addresses the Commission's concerns, the proposed modifications should be designed to effectively address the risks posed by transient devices to Low Impact BES Cyber Systems in a manner that is consistent with the risk-based approach reflected in the CIP version 5 Standards."*

SAR Information
• *Per paragraph 53, "…the Commission concludes that modifications to CIP-006-6 to provide controls to protect, at a minimum, communication links and data communicated between bulk electric system Control Centers are necessary in light of the critical role Control Center communications play in maintaining bulk electric system reliability. Therefore, we adopt the NOPR proposal and direct that NERC, pursuant to section 215(d)(5) of the FPA, develop modifications to the CIP Reliability Standards to require responsible entities to implement controls to protect, at a minimum, communication links and sensitive bulk electric system data communicated between bulk electric system Control Centers in a manner that is appropriately tailored to address the risks posed to the bulk electric system by the assets being protected (i.e., high, medium, or low impact)."* • *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 to provide the needed clarity, within one year of the effective date of this Final Rule…."* In addition, the SDT will review and address the CIP V5 requirements for CIP Exceptional Circumstances exceptions. Finally, the SDT will review the Guidelines and Technical Basis sections of the CIP V5 standards and adjust where appropriate as well as correct any grammatical, punctuation, and/or formatting errors, and make other errata changes to the CIP V5 standards, as necessary.

Reliability Functions	
The Standard will Apply to the Following Functions (Check each one that applies.)	
☐ Regional Reliability Organization	Conducts the regional activities related to planning and operations, and coordinates activities of Responsible Entities to secure the reliability of the Bulk Electric System within the region and adjacent regions.
☒ Reliability Coordinator	Responsible for the real-time operating reliability of its Reliability Coordinator Area in coordination with its neighboring Reliability Coordinator's wide area view.

Reliability Functions	
☒ Balancing Authority	Integrates resource plans ahead of time, and maintains load-interchange-resource balance within a Balancing Authority Area and supports Interconnection frequency in real time.
☒ Interchange Authority	Ensures communication of interchange transactions for reliability evaluation purposes and coordinates implementation of valid and balanced interchange schedules between Balancing Authority Areas.
☐ Planning Coordinator	Assesses the longer-term reliability of its Planning Coordinator Area.
☐ Resource Planner	Develops a >one year plan for the resource adequacy of its specific loads within a Planning Coordinator area.
☐ Transmission Planner	Develops a >one year plan for the reliability of the interconnected Bulk Electric System within its portion of the Planning Coordinator area.
☐ Transmission Service Provider	Administers the transmission tariff and provides transmission services under applicable transmission service agreements (e.g., the pro forma tariff).
☒ Transmission Owner	Owns and maintains transmission facilities.
☒ Transmission Operator	Ensures the real-time operating reliability of the transmission assets within a Transmission Operator Area.
☒ Distribution Provider	Delivers electrical energy to the End-use customer.
☒ Generator Owner	Owns and maintains generation facilities.
☒ Generator Operator	Operates generation unit(s) to provide real and Reactive Power.
☐ Purchasing-Selling Entity	Purchases or sells energy, capacity, and necessary reliability-related services as required.
☐ Market Operator	Interface point for reliability functions with commercial functions.
☐ Load-Serving Entity	Secures energy and transmission service (and reliability-related services) to serve the End-use Customer.

Reliability and Market Interface Principles		
Applicable Reliability Principles (Check all that apply).		
☐	1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.	
☐	2. The frequency and voltage of interconnected bulk power systems shall be controlled within defined limits through the balancing of real and Reactive Power supply and demand.	
☐	3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.	
☐	4. Plans for emergency operation and system restoration of interconnected bulk power systems shall be developed, coordinated, maintained and implemented.	
☒	5. Facilities for communication, monitoring and control shall be provided, used and maintained for the reliability of interconnected bulk power systems.	
☐	6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions.	
☐	7. The security of the interconnected bulk power systems shall be assessed, monitored and maintained on a wide area basis.	
☒	8. Bulk power systems shall be protected from malicious physical or cyber attacks.	
Does the proposed Standard comply with all of the following Market Interface Principles?		Enter (yes/no)
1. A reliability standard shall not give any market participant an unfair competitive advantage.		YES
2. A reliability standard shall neither mandate nor prohibit any specific market structure.		YES
3. A reliability standard shall not preclude market solutions to achieving compliance with that standard.		YES
4. A reliability standard shall not require the public disclosure of commercially sensitive information. All market participants shall have equal opportunity to access commercially non-sensitive information that is required for compliance with reliability standards.		YES

Related Standards	
Standard No.	Explanation

Related Standards	

Related SARs	
SAR ID	Explanation

Regional Variances	
Region	Explanation
FRCC	
MRO	
NPCC	
RF	
SERC	
SPP RE	
Texas RE	
WECC	

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Authorization Request Form

When completed, email this form to:
sarcomm@nerc.com

NERC welcomes suggestions to improve the reliability of the bulk power system through improved reliability standards. Please use this form to submit your request to propose a new or a revision to a NERC's Reliability Standard.

Request to propose a new or a revision to a Reliability Standard			
Title of Proposed Standard(s):	Modifications to CIP Standards		
Date Submitted:	~~March 9~~June 1, 2016		
SAR Requester Information			
Name:	Stephen Crutchfield		
Organization:	NERC		
Telephone:	609-651-9455	E-mail:	Stephen.Crutchfield@nerc.net
SAR Type (Check as many as applicable)			
☒ New Standard		☒ Withdrawal of existing Standard	
☒ Revision to existing Standard		☐ Urgent Action	

SAR Information
Purpose (Describe what the standard action will achieve in support of Bulk Electric System reliability.):
The purpose of this project is to (1) consider the Version 5 Transition Advisory Group (V5TAG) issues identified in the *CIP V5 Issues for Standard Drafting Team Consideration* (V5TAG Transfer Document) and (2) address the Federal Energy Regulatory Commission (Commission) directives contained in Order 822. These revisions will increase reliability and security to the Bulk-Power System (BPS) by enhancing cyber protection of BPS facilities.
Industry Need (What is the industry problem this request is trying to solve?):
The V5TAG, which consists of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP ~~version 5~~V5 standards and to support industry's implementation activities. During the course of the V5TAG's activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by the existing standard drafting team (SDT) for the CIP Reliability Standards.

SAR Information

The V5-TAG developed the V5TAG Transfer Document to explain the issues and recommend that the SDT consider them in future development activity.

On January 21, 2016, the Commission issued Order No. 822 approving revisions to the CIP version 5 standards and also directing NERC to develop modifications to address:

- Protection of transient electronic devices used at low-impact BES Cyber Systems;
- Protections for communication network components between control centers; and
- Refinement of the Low Impact External Routable Connectivity (LERC) definition.

The Commission did not provide a date by which the modifications for transient devices or communication networks must be completed. For the LERC definition, however, the Commission directed that NERC submit the modification within one year of the effective date of Order No. 822 (March 31, 2017).

Brief Description (Provide a paragraph that describes the scope of this standard action.)

The proposed project will consider the issues raised by the V5TAG in the V5TAG Transfer Document and will address the Commission directives in Order No. 822 through modifications to the CIP standards. The work will include development of Violation Risk Factors, Violation Severity Levels, and an Implementation Plan for the modified standards and will meet the deadlines established by the Commission in Order No. 822.

Detailed Description (Provide a description of the proposed project with sufficient details for the standard drafting team to execute the SAR. Also provide a justification for the development or revision of the standard, including an assessment of the reliability and market interface impacts of implementing or not implementing the standard action.)

As stated above, the purpose of this project is to consider the V5TAG issues in the initial transfer document V5TAG Transfer Document and address the Commission directives contained in Order 822. For the directive on the LERC definition, the project is to respond within the deadline required in the order.

As noted above, the V5TAG identified specific issues with the CIP V5 standards. The V5TAG drafted the V5TAG Transfer Document to formally recommend that the SDT address these issues during standards development to consider whether modifications can be made to the standard language. As outlined in the V5TAG Transfer Document, the specific issues are as follows:

- 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. The V5TAG recommends the following enhancements:
    - Clarify the intent of “programmable” in Cyber Asset.
    - Clarify and focus the definition of “BES Cyber Asset” including:

SAR Information

- 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.

- 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"
  - The meaning of the word 'associated' in the ERC definition.
  - The applicability of ERC including the concept of the term "directly" used in the phrase "cannot be directly accessed through External Routable Connectivity" within the Applicability section.
  - The IRA definition placement of the phrase "using a routable protocol" in the definition and with respect to Dial-up Connectivity.
  - The Guidelines and Technical Basis sentence, "If dial-up connectivity is used for Interactive Remote Access, then Requirement R2 also applies."
- Transmission Owner (TO) Control Centers Performing Transmission Operator (TOP) Obligations – V5TAG is aware of multiple interpretations of the language "used to perform the functional obligation of" in CIP-002-5.1 Attachment 1, section 2.12 and recommends clarification of:
  - The applicability of requirements on a TO Control Center that performs the functional obligations of a TOP, particularly if the TO has the ability to operate switches, breakers and relays in the BES.
  - The definition of Control Center.
  - The language scope of "perform the functional obligations of" throughout the Attachment 1 criteria.
- Virtualization – The CIP V5 standards do not specifically address virtualization. Because of the increasing use of virtualization in industrial control system environments, V5TAG asked that the SDT consider the CIP ~~005~~ V5 standards and the associated definitions ~~of Cyber Asset and Electronic Access Point~~ regarding permitted architecture and the security risks of ~~network, server and storage~~ virtualization technologies.

The SDT shall also address the Order No. 822 directives by developing modifications to requirements in CIP standards and the definition of LERC. The Commission directed the following:

- *Per paragraph 32, "...we direct that NERC, pursuant to section 215(d)(5) of the FPA, develop modifications to the CIP Reliability Standards to provide mandatory protection for transient devices used at Low Impact BES Cyber Systems based on the risk posed to bulk electric system reliability. While NERC has flexibility in the manner in which it addresses the Commission's concerns, the proposed modifications should be designed to effectively address the risks posed by*

SAR Information
transient devices to Low Impact BES Cyber Systems in a manner that is consistent with the risk-based approach reflected in the CIP version 5 Standards." • *Per paragraph 53, "…the Commission concludes that modifications to CIP-006-6 to provide controls to protect, at a minimum, communication links and data communicated between bulk electric system Control Centers are necessary in light of the critical role Control Center communications play in maintaining bulk electric system reliability. Therefore, we adopt the NOPR proposal and direct that NERC, pursuant to section 215(d)(5) of the FPA, develop modifications to the CIP Reliability Standards to require responsible entities to implement controls to protect, at a minimum, communication links and sensitive bulk electric system data communicated between bulk electric system Control Centers in a manner that is appropriately tailored to address the risks posed to the bulk electric system by the assets being protected (i.e., high, medium, or low impact)."* • *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 to provide the needed clarity, within one year of the effective date of this Final Rule…."* In addition, the SDT will review and address the CIP V5 requirements for CIP Exceptional Circumstances exceptions. Finally, the SDT will review the Guidelines and Technical Basis sections of the CIP V5 standards and adjust where appropriate as well as correct any grammatical, punctuation, and/or formatting errors, and make other errata changes to the CIP V5 standards, as necessary.

Reliability Functions	
The Standard will Apply to the Following Functions (Check each one that applies.)	
☐ Regional Reliability Organization	Conducts the regional activities related to planning and operations, and coordinates activities of Responsible Entities to secure the reliability of the Bulk Electric System within the region and adjacent regions.
☒ Reliability Coordinator	Responsible for the real-time operating reliability of its Reliability Coordinator Area in coordination with its neighboring Reliability Coordinator's wide area view.

Reliability Functions	
☒ Balancing Authority	Integrates resource plans ahead of time, and maintains load-interchange-resource balance within a Balancing Authority Area and supports Interconnection frequency in real time.
☒ Interchange Authority	Ensures communication of interchange transactions for reliability evaluation purposes and coordinates implementation of valid and balanced interchange schedules between Balancing Authority Areas.
☐ Planning Coordinator	Assesses the longer-term reliability of its Planning Coordinator Area.
☐ Resource Planner	Develops a >one year plan for the resource adequacy of its specific loads within a Planning Coordinator area.
☐ Transmission Planner	Develops a >one year plan for the reliability of the interconnected Bulk Electric System within its portion of the Planning Coordinator area.
~~☒~~ ☐ Transmission Service Provider	Administers the transmission tariff and provides transmission services under applicable transmission service agreements (e.g., the pro forma tariff).
☒ Transmission Owner	Owns and maintains transmission facilities.
☒ Transmission Operator	Ensures the real-time operating reliability of the transmission assets within a Transmission Operator Area.
~~☐~~ ☒ Distribution Provider	Delivers electrical energy to the End-use customer.
☒ Generator Owner	Owns and maintains generation facilities.
☒ Generator Operator	Operates generation unit(s) to provide real and Reactive Power.
☐ Purchasing-Selling Entity	Purchases or sells energy, capacity, and necessary reliability-related services as required.
☐ Market Operator	Interface point for reliability functions with commercial functions.
☐ Load-Serving Entity	Secures energy and transmission service (and reliability-related services) to serve the End-use Customer.

Reliability and Market Interface Principles		
Applicable Reliability Principles (Check all that apply).		
☐	1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.	
☐	2. The frequency and voltage of interconnected bulk power systems shall be controlled within defined limits through the balancing of real and Reactive Power supply and demand.	
☐	3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.	
☐	4. Plans for emergency operation and system restoration of interconnected bulk power systems shall be developed, coordinated, maintained and implemented.	
☒	5. Facilities for communication, monitoring and control shall be provided, used and maintained for the reliability of interconnected bulk power systems.	
☐	6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions.	
☐	7. The security of the interconnected bulk power systems shall be assessed, monitored and maintained on a wide area basis.	
☒	8. Bulk power systems shall be protected from malicious physical or cyber attacks.	
Does the proposed Standard comply with all of the following Market Interface Principles?		Enter (yes/no)
1. A reliability standard shall not give any market participant an unfair competitive advantage.		YES
2. A reliability standard shall neither mandate nor prohibit any specific market structure.		YES
3. A reliability standard shall not preclude market solutions to achieving compliance with that standard.		YES
4. A reliability standard shall not require the public disclosure of commercially sensitive information. All market participants shall have equal opportunity to access commercially non-sensitive information that is required for compliance with reliability standards.		YES

Related Standards	
Standard No.	Explanation

Related Standards	

Related SARs	
SAR ID	Explanation

Regional Variances	
Region	Explanation
FRCC	
MRO	
NPCC	
RF	
SERC	
SPP RE	
Texas RE	
WECC	

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Comment Form

Project 2016-02 Modifications to CIP Standards Standards Authorization Request (SAR)

Do not use this form for submitting comments. Use the electronic form to submit comments on the **Project 2016-02 Modifications to CIP Standards SAR**. The electronic comment form must be submitted by **8 p.m. Eastern, Thursday, June 30, 2016**.

Additional information about this project is available on the Project 2016-02 Modifications to CIP Standards page. If you have questions, contact either Senior Standards Developer, Stephen Crutchfield at (609) 651-9455 or Al McMeekin at (404) 446-9675.

Background Information

On January 21, 2016, the Commission issued Order No. 822, *Revised Critical Infrastructure Protection Reliability Standards,* approving seven CIP Reliability Standards and new or modified definitions. On March 9, 2016, the NERC Standards Committee accepted the Standards Authorization Request (SAR) and authorized the posting of the Modifications to CIP Standards SAR. It was posted for a 30-day informal comment period March 23 – April 21, 2016. Based on the comments received, the Standard Drafting Team (SDT) made minor revisions to the SAR which will be posted for an additional 30-day informal comment period.

It was noted in the comments received on the SAR that the Virtualization issue involved more than just CIP-005 standards and the defined terms Cyber Asset and Electronic Access Point. To correct this, the SDT revised the sentence to: "Because of the increasing use of virtualization in industrial control system environments, V5TAG asked that the SDT consider ~~CIP-005 and the definitions of Cyber Asset and Electronic Access Point~~ the CIP V5 standards and the associated definitions regarding permitted architecture and the security risks of ~~network, server and storage~~ virtualization technologies."

Other commenters suggested that the SDT include provisions to address CIP Exceptional Circumstances. A sentence was added to the SAR to include this topic: "In addition, the SDT will review and address the CIP V5 requirements for CIP Exceptional Circumstances exceptions."

A sentence was also added to the SAR allowing the SDT to make errata changes to the standards as necessary and to correct grammatical, punctuation and/or formatting errors in the V5 Standards: "Finally, the SDT will review the Guidelines and Technical Basis sections of the CIP V5 standards and adjust where appropriate as well as correct any grammatical, punctuation, and/or formatting errors, and make other errata changes to the CIP V5 standards, as necessary."

In the previous version of the SAR, the Transmission Service Provide (TSP) Reliability Function was checked as an applicable function. The TSP is not applicable under the CIP standards and this function was corrected by unchecking the TSP Reliability Function in this version of the SAR. Similarly, the Distribution

Provider (DP) Reliability Function was left unchecked in the original SAR. The CIP Standards apply to the DP, so this was corrected by checking the DP Reliability Function in this version of the SAR.

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.

   Yes:

   No:

   Comments:

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP V5 Issues for Standard Drafting Team Consideration

September 15, 2015

From experience in the V5 Transition Study and the on-going implementation efforts, the CIP Version 5 Transition Advisory Group (V5TAG) identified specific issues with the CIP Version 5 standard language that caused difficulty in implementation of the requirements. In many cases, the V5TAG members found that select language within the CIP Version 5 standards may be understood in multiple ways. These interpretations appear to go beyond the intended flexibility of the standard language that is necessary to accommodate the diverse nature of facts and circumstances across the electric sector. At this time, the V5TAG proposes the following issues to be addressed by the CIP V5 Revisions drafting team (SDT) or other appropriate team for standards development:

- **Cyber Asset and BES Cyber Asset definitions**

  The foundational definition for the CIP Version 5 standards is 'Cyber Assets.' When Cyber Assets meet a threshold of Bulk Electric System (BES) impact they become 'BES Cyber Assets (BCA)' which are grouped, by a Responsible Entity, into 'BES Cyber Systems (BCS).' Viewing BCAs too broadly can lead to many thousands of devices in the typical utility becoming an administrative burden for which few if any cyber security controls can actually be applied or where there is limited associated cyber security risk. Vast amounts of effort would be expended for these types of cyber assets to track and document their lack of capability for even the most basic cyber security controls. Viewing BCAs too narrowly could lead to missing consideration of devices that have a sufficient level of cyber capability and risk impact.

  The SDT should consider the definition of Cyber Asset and clarify the intent of "programmable" by considering such factors as if a device is merely configurable, its executable code is not field upgradable, or if its functionality can only be changed via physical DIP switches, swapping internal chips, etc.

  The SDT should consider clarifying and focusing the definition of "BES Cyber Asset" including:

  a. Focusing the definition so that it does not subsume all other cyber asset types. Protected Cyber Assets (PCA), by nature of being on the same network, can have some form of adverse impact if misused. Electronic Access Control or Monitoring Systems (EACMS) if misused or unavailable can have some form of adverse impact. This can result in a "hall of

mirrors" effect where everything in or that creates an Electronic Security Perimeter (ESP) also meets the BCA definition.

b. Considering if there is a lower bound to the term 'adverse' in "adverse impact". For example, is the focus of a typical generating unit the servers and operator human machine interfaces (HMI) and controller cabinets and Programmable Logic Controllers (PLCs) or is it the thousands of individual sensors and transmitters throughout the plant?

c. Clarify 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.

- **Network and Externally Accessible Devices (ERC, ESP, IRA)**

  The SDT should consider the concepts and requirements concerning Electronic Security Perimeters (ESP), External Routable Connectivity (ERC), and Interactive Remote Access (IRA) including:

  a. Clarify 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.

  b. The word 'associated' in the ERC definition is unclear in that it alludes to some form of relationship but does not define the relationship between the items. Striking 'associated' and defining the intended relationship would provide much needed clarity.

  c. Review of the applicability of ERC including the concept of the term "directly" used in the phrase "cannot be directly accessed through External Routable Connectivity" within the Applicability section. As well, consider the interplay between IRA and ERC.

  d. Clarify the IRA definition to address the placement of the phrase "using a routable protocol" in the definition and clarity with respect to Dial-up Connectivity.

  e. Address the Guidelines and Technical Basis sentence, "If dial-up connectivity is used for Interactive Remote Access, then Requirement R2 also applies."

- **Transmission Owner (TO) Control Centers Performing Transmission Operator (TOP) Obligations**

  CIP-002-5.1 Attachment 1 – Impact Reliability Criteria, sections 1.1, 1.2, 1.3, 1.4, 2.11, 2.12, and 2.13 employ the language "used to perform the functional obligation of", and then lists the functional registration. It was intended that this caveat would capture entities that perform obligations of a specific registered function, whether they are registered for that function or not. However, this language has caused confusion, especially in section 2.12 concerning TOP Control Centers. The term "functional obligation" may be interpreted to have different meaning in a variety of situations.

One interpretation is for the defined term Control Center to be strictly associated with the Balancing Authority (BA), Generator Operator (GOP), Reliability Coordinator (RC), and Transmission Operator (TOP) functional registrations, and that control rooms or dispatch centers owned and operated by Transmission Owners (TOs) with control of limited BES facilities would be excluded. A second interpretation may expand or contract the applicability of the Control Center designation, based on criteria that may not take into consideration overall risk to reliable operations of the BES.

Early analysis found the potential for TOs (not Registered as TOPs) that only operate limited breakers to be pulled in as medium impact Control Centers, even if the few Facilities they control are low impact. (For example, an entity with one 161kV breaker in one substation and a second 161kV breaker in a different substation, both breakers associated with low impact Facilities.) As currently written, low impact Control Centers are to be identified per criteria 3.1 and could be commensurate with risk for these scenarios.

Areas for the SDT to address are:

a. CIP-002-5.1, Attachment 1 Control Center criteria for additional clarity and for possible revisions related to TOP or TO Control Centers performing the functional obligations of a TOP, in particular for small or lower-risk entities. A potential revision could be a size for criteria 2.12, Control Centers performing the functional obligations of a TOP.
b. Clarify the applicability of requirements on a TO Control Center that perform the functional obligations of a TOP, particularly if the TO has the ability to operate switches, breakers and relays in the BES. Review the corresponding Guidelines and Technical Basis of CIP-002-5.1, specifically: the "CIP-002-5" section paragraph starting with "Responsibility for the reliable operation of the BES is spread across all Entity Registrations"; the table following that paragraph; the "High Impact Rating (H)" section; and the criterion bullets for Control Centers under the "Medium Impact Rating (M)" section.
c. The definition of Control Center (if pursued, recognize possible impacts on operations and planning standards and/or glossary terms that include 'Control Center', for example, the revised Glossary term for "System Operator" to be effective July 1, 2016).
d. The language scope of "perform the functional obligations of" throughout the Attachment 1 criteria.

- **<u>Virtualization</u>**

  The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration.

The SDT should consider revisions to CIP-005 and the definitions of Cyber Asset and Electronic Access Point that make clear the permitted architecture and address the security risks of network, server and storage virtualization technologies.

The transition to CIP Version 5 continues as the compliance deadline of April 1, 2016 approaches. The V5TAG continues to discuss challenging issues being undertaken during the on-going implementation. The group may find additional issues to transfer to the SDT for consideration.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2016-02 Modifications to CIP Standards Standards Authorization Request

Informal Comment Period Open through June 30, 2016

Now Available

A 30-day informal comment period for the **Project 2016-02 Standards Authorization Request (SAR)**, is open through **8 p.m. Eastern, Thursday, June 30, 2016**.

Commenting

Use the electronic form to submit comments on the SAR. If you experience any difficulties in using the electronic form, contact Wendy Muller. An unofficial Word version of the comment form is posted on the project page.

If you are having difficulty accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out, contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 8 p.m. Eastern).

Next Steps

The drafting team will review all responses received during the comment period and determine the next steps of the project

For more information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact either Senior Standards Developer, Stephen Crutchfield at (609) 651-9455 or Al McMeekin at (404) 446-9675.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

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 Hils	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 dradting 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’ wheras 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 Oder 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	

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.

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.

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.

Changes to SAR Redlined Language

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

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

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Posting Document / Unofficial Comment Form

Project 2016-02 Modifications to CIP Standards Communication Networks

Do not use this form for submitting comments. Use the electronic form to submit comments on the Standard Drafting Team's (SDT) approach and draft language **to address the Federal Energy Regulatory Commission (Commission or FERC) directive regarding Communication Networks**. The electronic form must be submitted by **8 p.m. Eastern, March 13, 2017.**

To minimize the number of posted documents, the SDT included everything in this single document with the questions following the suggested approach and draft language.

Additional information is available on the project page. If you have questions, contact Senior Standards Developer, Al McMeekin (via email) or at (404) 446-9675.

Introduction

On January 21, 2016, the Commission issued Order No. 822 approving seven CIP Reliability Standards and new or modified definitions and issuing certain directives requesting modifications to the CIP Reliability Standards. The focus of this informal comment period is on the directive from the Commission requesting NERC to "develop modifications to the CIP Reliability Standards to require responsible entities to implement controls to protect, at a minimum, communication links and sensitive bulk electric system data communicated between bulk electric system Control Centers in a manner that is appropriately tailored to address the risks posed to the bulk electric system by the assets being protected (i.e., high, medium, or low impact)." (Order 822, Paragraph 53)

The SDT is working through an evaluation process to determine appropriate actions to take in order to meet the Commission's directive. The informal posting reflected herein represents the initial exploratory efforts to research the scope and objectives of the draft standard and associated requirements. The SDT will consider all comments received from industry stakeholders and will revise the draft language accordingly. The revised language may expand in scope and the security objective(s) may be modified to align with industry comments.

The SDT is considering the following assumptions and is requesting stakeholder input through the comment form below on the validity of these assumptions:

- A formal definition of "sensitive BES data" is not required because Responsible Entities are already required to identify operational reliability data in FERC-approved Reliability Standards TOP-003-3 and IRO-010-2.
- Data at rest within a BES Cyber System is already afforded protections in existing CIP standards (CIP-003, 005, 007, etc.), is perishable, and has a diminished need for protection over time.

- The existing definition of Control Center is adequate.

In addressing the directive, the SDT's initial efforts are focused specifically on the communication links transmitting sensitive data between Control Centers. While the directive language in Order 822 specifically references modifications to CIP-006-6 which handles physical security controls, the SDT is considering language around logical protections of these communication links through a programmatic approach. Because these requirements will apply to Control Centers at all impact levels (high, medium, and low), the SDT is also proposing to create a new CIP Reliability Standard, CIP-012-1, to address the protection of sensitive BES data transmitted between Control Centers. While the SDT is not yet certain of the full scope of requirements necessary to address the directive found in paragraph 53 of Order 822. Some of the draft language the SDT is currently considering and requesting stakeholder feedback on is as follows.

Draft Language

The Responsible Entity shall implement one or more documented plan(s) that achieve the security objective to protect confidentiality and integrity[1] of data required for reliable operation of the BES. The plan applies to data being transferred across communication networks between Control Centers, both inter-entity and intra-entity and shall include each of the applicable parts below:

1.1 Procedure(s) to identify the communication networks requiring protections;

1.2 Procedure(s) for defining the boundaries of communication networks transmitting data required for reliable operation identified in 1.1, if applicable;

1.3 Method(s) for protecting communication networks between Control Centers identified in 1.1, where technically feasible.

Examples of evidence may include, but are not limited to, plan documents; documentation such as representative diagrams, configuration settings or demonstration materials to illustrate and verify that confidentiality and integrity of data transmitted between Control Centers has been protected and satisfies the security objective. Information gathering during walk-downs or visual inspections can validate the implementation of necessary controls. The documentation as referenced may be used to further validate where protections may or may not be required.

Draft Guidance

This draft language mandates that communication networks required for reliable operation between Control Centers be identified and protected. The Responsible Entity has flexibility in determining how to implement the draft language.

In developing plan(s), the number of plan(s) and their content should be guided by a Responsible Entity's management structure and operating conditions. Each Responsible Entity is required to implement one or more documented plan(s) that achieve the stated security objective of protecting the

[1] NIST Special Publication 800-53A : Revision 4, Appendix B : http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf

confidentiality and integrity of data that is required for reliable operation and is transmitted between Control Centers. To achieve this objective, the Responsible Entity is required to document and implement plan(s) that include a procedure(s) for the identification of communication networks that transmit operational reliability data between Control Centers. The plan(s) should identify the applicable communication networks both within the entity's footprint, and any applicable networks between Responsible Entities. When defining the procedures for identifying applicable communication networks, the Responsible Entity should ensure that the methods chosen include rationale supporting the identification of such communication networks. As one possible solution, the Responsible Entity could apply CIP-002 criteria to identify all inter-Control Center and intra-Control Center communication links that could adversely impact the reliable operation of the Control Center within 15 minutes. Another possible solution to identifying in-scope communication networks is to take a data-centric approach. The Responsible Entity could identify applicable operational reliability data that is transmitted between Control Centers. This data has already been identified for some applicable entities (Reliability Coordinator (RC) and Transmission Operator (TOP)) in the data specification requirements. Responsible Entities such as the Distribution Provider (DP) and Generator Operator (GOP) that do not have existing data specification requirements should identify, at a minimum, operational reliability data that has been requested by a Balancing Authority (BA), RC, or TOP as operational reliability data.
The Responsible Entity could then use the data identified in the previous step to determine which communication links require protection under CIP-12-1. Examples of these communication links are:

1. Data link(s) between neighboring Transmission Operators
2. Data link(s) between a Balancing Authority and a Reliability Coordinator
3. Data link(s) between a Generator Operator and a Balancing Authority
4. Data link(s) between a Transmission Owner and a Transmission Operator
5. Data link(s) between a Distribution Provider and a Transmission Operator
6. Data link(s) between Reliability Coordinators
7. Data link(s) between two Primary Control Centers owned by a Responsible Entity
8. Data link(s) between a Primary and Backup Control Center owned by a Responsible Entity

The plan(s) should address how the boundary is determined for all communication networks that are identified using the entity-developed procedure(s) (e.g. ESP boundary, Router outside of an ESP but within a PSP, Cyber Asset used as an electronic access control for a low impact BES Cyber System, etc.). A Responsible Entity has the freedom to identify these boundaries as it sees fit. The entity should take the various features of its environment into account and determine the most effective and efficient solution when defining these boundaries. There is no limitation on where boundary protection must begin and terminate, other than ensuring that the endpoint identified is controlled by the Responsible Entity. The SDT recommends that when selecting the endpoint, Responsible Entities carefully consider reliability concerns and technical limitations. Endpoints identified by the Responsible Entity are not meant to represent additional assets to be included in the scope of the CIP Reliability Standards. The intent of the endpoint identification is to ensure each Responsible Entity identifies clear demarcation of where the protections applied to the in-scope communications networks exist. The boundaries can vary

based upon impact levels of the Control Center containing BES Cyber Systems, different technologies, or infrastructures. The list of example network boundaries is provided below:

- Electronic Access Point on the Electronic Security Perimeter boundary of a High or Medium Impact BES Cyber System
- Router outside of an Electronic Security Perimeter that is protected under an Entity's Physical Security Program
- A Cyber Asset that performs the role of an Electronic Access Control for a low impact BES Cyber System

Additionally, the Responsible Entity must document and implement plans for the protection of the confidentiality and integrity of operational reliability data communicated between Control Centers. This security objective could be achieved through a variety of methods or combination of methods (e.g. site to site encryption, application layer encryption, physical protection, etc.). The methods must address the confidentiality and integrity of the operational reliability data and protect the data on the applicable communication networks/data links between Control Centers. The protections to be applied to the communication links identified by the Responsible Entity are chosen at the Responsible Entity's discretion. However, the Responsible Entity should exercise caution to ensure that both confidentiality and integrity of the in-scope communication links are protected. Some examples of methods that can be implemented include but are not limited to:

- Site to site encryption: Site to site encryption provides a means to securely transmit and access information between two or more sites. Site to site encryption allows peers at both ends of the identified link to encrypt and decrypt packets using mutually agreed-upon keys or certificates and methods of encryption. This method can be used to achieve the protection of both the confidentiality and integrity of the communication link provided that the encryption method chosen not only obfuscates the data payload, but also provides a means to verify that the data payload did not change between the source and destination.
- Application layer encryption: Application-layer encryption protects the data at the highest layer in the BES cyber system providing the sensitive data, making it invisible to all the layers below. If a Responsible Entity chooses this option, care must be taken to ensure the inclusion of both confidentiality and integrity. If the solution implemented only addresses confidentiality, the Responsible Entity will need to also implement a complementary control, such as a hashing mechanism, to protect against the manipulation of the data.
- Physical protections: In some cases, a Responsible Entity may choose to implement physical protections on the communication links in question. Secure conduit can be a method to help secure the confidentiality and integrity of an in-scope link between Control Centers, as well as helping ensure availability. While this measure can be used, it is suggested that a Responsible Entity complement physical protections with logical protections to fully ensure that the integrity and confidentiality of data transmitted between Control Centers is protected.

Questions

1. The SDT asserts that the referenced data is already afforded protections at rest under existing CIP standards (CIP-003, 005, 007, etc.), is perishable, and has a diminished need for protection over time. Do you agree with the SDT's assertion? If you agree, please supply a rationale to support the position.

   ☐ Yes
   ☐ No

   Comments:

2. If you do not agree with the SDT's assertion in Question 1, please identify the type of data, the risk posed at rest, and supply the rationale to support the position.

   Comments:

3. Future enforceable Reliability Standards IRO-010-2 and TOP-003-3 identify "data required for reliable operation." For example, Requirement R1 of IRO-010-2 states:

   R1. The Reliability Coordinator shall maintain a documented specification for the data necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments. The data specification shall include but not be limited to:

   1.1. A list of data and information needed by the Reliability Coordinator to support its Operational Planning Analyses, Real-time monitoring, and Realtime Assessments including non-BES data and external network data, as deemed necessary by the Reliability Coordinator.

   TOP-003-3 Requirements R1 & R2 also have similar requirements for BAs and TOPs.

   Do you agree that outlining this approach for identifying "data required for reliable operation" in the Guidelines and Technical Basis is sufficient; consequently, an additional definition of "sensitive BES data" or a requirement to identify "sensitive BES data" is not necessary? If not, please explain.

   ☐ Yes
   ☐ No

   Comments:

4. The SDT asserts that "availability" of inter-and intra-entity Control Center communication of data is being addressed in Project 2016-01 Modifications to TOP and IRO Standards, specifically Reliability Standards TOP-001-4 and IRO-002-5. The proposed standards require redundant and diversely routed data exchange capabilities at a Responsible Entity's primary Control Center. Do you agree that "availability" is adequately addressed by these standards? If not, please provide rationale to support your position.

   ☐ Yes
   ☐ No

   Comments:

5. The SDT is proposing to develop a new CIP standard because the directives of FERC Order 822 related to the protection of communication networks used to exchange sensitive BES data regardless of the entity's size or impact level. Do you agree with the drafting of a new CIP standard to address this issue? If you disagree and would prefer to include requirements in existing CIP Standards, such as CIP-003 and CIP-005, please provide rationale and propose requirement language.

   ☐ Yes
   ☐ No

   Comments:

6. The SDT evaluated multiple approaches to addressing the directive. The approach proposed in this informal posting focuses on the protection of communication links. An alternative approach could focus on the protection of the sensitive BES data itself. Do you agree with the SDT's approach to focus the draft language on the protection of communication links? If not, please provide rationale and propose alternative language.

   ☐ Yes
   ☐ No

   Comments:

7. Do you agree with the security objective of the draft language? If not, please propose alternative language.

   ☐ Yes
   ☐ No

   Comments:

8. Is it clear what types of plans, procedures, and methods are needed to meet the draft language? If not, please propose alternative language.

   ☐ Yes
   ☐ No

   Comments:

9. The SDT uses the term "communication networks" throughout the draft language including an obligation to define the boundaries of such communication networks. Does the SDT need to define the term for inclusion in the NERC Glossary of Terms? If so, please propose a definition of "communication networks."

   ☐ Yes
   ☐ No

   Comments:

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

2016-02 Modifications to CIP Standards Communication Networks and CIP Exceptional Circumstances

Informal Comment Period Open through March 13, 2017

Now Available

The Project 2016-02 Standard Drafting Team (SDT) is requesting stakeholder input on two issues it is addressing: (1) the Federal Energy Regulatory Commission directive regarding Communication Networks; and, (2) determining if additional CIP requirements are impacted during a declared CIP Exceptional Circumstance. 30-day informal comment periods are open through **8 p.m. Eastern, Monday, March 13, 2017** for stakeholders to provide feedback on the SDT's approach and draft language for each issue. To minimize the number of posted documents, the SDT included everything in a single document for each issue with the suggested approach and draft language preceding the questions.

Commenting

Use the electronic form to submit comments. If you experience any difficulties using the electronic form, contact Wendy Muller.

If you are having difficulty accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out, contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern).

- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*
- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Next Steps

The drafting team will review all responses received during the informal comment period and determine the next steps of the project.

For more information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact Senior Standards Developer, Al McMeekin (via email) or at (404) 446-9675.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Comment Report

Project Name:	2016-02 Modifications to CIP Standards | Communication Networks
Comment Period Start Date:	2/10/2017
Comment Period End Date:	3/13/2017
Associated Ballots:	

There were 48 sets of responses, including comments from approximately 121 different people from approximately 91 companies representing 10 of the Industry Segments as shown in the table on the following pages.

Questions

1. The SDT asserts that the referenced data is already afforded protections at rest under existing CIP standards (CIP-003, 005, 007, etc.), is perishable, and has a diminished need for protection over time. Do you agree with the SDT's assertion? If you agree, please supply a rationale to support the position.

2. If you do not agree with the SDT's assertion in Question 1, please identify the type of data, the risk posed at rest, and supply the rationale to support the position.

3. Future enforceable Reliability Standards IRO-010-2 and TOP-003-3 identify "data required for reliable operation." For example, Requirement R1 of IRO-010-2 states:

R1. The Reliability Coordinator shall maintain a documented specification for the data necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and

1.1. A list of data and information needed by the Reliability Coordinator to support its Operational Planning Analyses, Real-time monitoring, and Realtime Assessments including non-BES data

TOP-003-3 Requirements R1 & R2 also have similar requirements for BAs and TOPs.

Do you agree that outlining this approach for identifying "data required for reliable operation" in the Guidelines and Technical Basis is sufficient; consequently, an additional definition of "sensitive BES data" or a requirement to identify "sensitive BES data" is not necessary? If not, please explain.

4. The SDT asserts that "availability" of inter-and intra-entity Control Center communication of data is being addressed in Project 2016-01 Modifications to TOP and IRO Standards, specifically Reliability Standards TOP-001-4 and IRO-002-5. The proposed standards require redundant and diversely routed data exchange capabilities at a Responsible Entity's primary Control Center. Do you agree that "availability" is adequately addressed by these standards? If not, please provide rationale to support your position.

5. The SDT is proposing to develop a new CIP standard because the directives of FERC Order 822 related to the protection of communication networks used to exchange sensitive BES data regardless of the entity's size or impact level. Do you agree with the drafting of a new CIP standard to address this issue? If you disagree and would prefer to include requirements in existing CIP Standards, such as CIP-003 and CIP-005, please provide rationale and propose requirement language.

6. The SDT evaluated multiple approaches to addressing the directive. The approach proposed in this informal posting focuses on the protection of communication links. An alternative approach could focus on the protection of the sensitive BES data itself. Do you agree with the SDT's approach to focus the draft language on the protection of communication links? If not, please provide rationale and propose alternative language.

7. Do you agree with the security objective of the draft language? If not, please propose alternative language.

8. Is it clear what types of plans, procedures, and methods are needed to meet the draft language? If not, please propose alternative language.

9. The SDT uses the term "communication networks" throughout the draft language including an obligation to define the boundaries of such communication networks. Does the SDT need to define the term for inclusion in the NERC Glossary of Terms? If so, please propose a definition of "communication networks."

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
Tennessee Valley Authority	Brian Millard	1,3,5,6	SERC	Tennessee Valley Authority	Scott, Howell D.	Tennessee Valley Authority	1	SERC
					Grant, Ian S.	Tennessee Valley Authority	3	SERC
					Thomas, M. Lee	Tennessee Valley Authority	5	SERC
					Parsons, Marjorie S.	Tennessee Valley Authority	6	SERC
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
Seattle City Light	Ginette Lacasse	1,3,4,5,6	WECC	Seattle City Light Ballot Body	Pawel Krupa	Seattle City Light	1	WECC
					Hao Li	Seattle City Light	4	WECC
					Bud (Charles) Freeman	Seattle City Light	6	WECC
					Mike Haynes	Seattle City Light	5	WECC
					Michael Watkins	Seattle City Light	1,4	WECC
					Faz Kasraie	Seattle City Light	5	WECC
					John Clark	Seattle City Light	6	WECC
					Tuan Tran	Seattle City Light	3	WECC
					Laurrie Hammack	Seattle City Light	3	WECC

Entergy	Julie Hall	6		Entergy/NERC Compliance	Oliver Burke	Entergy - Entergy Services, Inc.	1	SERC
					Jaclyn Massey	Entergy - Entergy Services, Inc.	5	SERC
DTE Energy - Detroit Edison Company	Karie Barczak	3,4,5		DTE Energy - DTE Electric	Jeffrey Depriest	DTE Energy - DTE Electric	5	RF
					Daniel Herring	DTE Energy - DTE Electric	4	RF
					Karie Barczak	DTE Energy - DTE Electric	3	RF
Con Ed - Consolidated Edison Co. of New York	Kelly Silver	1,3,5,6	NPCC	Con Edison	Kelly Silver	Con Edison Company of New York	1,3,5,6	NPCC
					Edward Bedder	Orange and Rockland Utilities	NA - Not Applicable	NPCC
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,8,9,10	NPCC	RSC no Dominion	Paul Malozewski	Hydro One.	1	NPCC
					Guy Zito	Northeast Power Coordinating Council	NA - Not Applicable	NPCC
					Randy MacDonald	New Brunswick Power	2	NPCC
					Wayne Sipperly	New York Power Authority	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	Orange & Rockland Utilities	3	NPCC
					Michele Tondalo	UI	1	NPCC
					Sylvain Clermont	Hydro Quebec	1	NPCC
					Si Truc Phan	Hydro Quebec	2	NPCC
					Helen Lainis	IESO	2	NPCC
					Laura Mcleod	NB Power	1	NPCC
					MIchael Forte	Con Edison	1	NPCC
					Kelly Silver	Con Edison	3	NPCC
					Peter Yost	Con Edison	4	NPCC
					Brian O'Boyle	Con Edison	5	NPCC
					Greg Campoli	NY-ISO	2	NPCC
					Kathleen Goodman	ISO-NE	2	NPCC
					Michael Schiavone	National Grid	1	NPCC
					Michael Jones	National Grid	3	NPCC
					David Ramkalawan	Ontario Power Generation Inc.	5	NPCC
					Quintin Lee	Eversource Energy	1	NPCC
					Silvia Mitchell	NextEra Energy - Florida Power and Light Co.	6	NPCC
Midwest Reliability Organization	Russel Mountjoy	10		MRO NSRF	Joseph DePoorter	Madison Gas & Electric	3,4,5,6	MRO
					Larry Heckert	Alliant Energy	4	MRO
					Amy Casucelli	Xcel Energy	1,3,5,6	MRO

					Chuck Lawrence	American Transmission Company	1	MRO
					Michael Brytowski	Great River Energy	1,3,5,6	MRO
					Jodi Jensen	Western Area Power Administratino	1,6	MRO
					Kayleigh Wilkerson	Lincoln Electric System	1,3,5,6	MRO
					Mahmood Safi	Omaha Public Power District	1,3,5,6	MRO
					Brad Parret	Minnesota Power	1,5	MRO
					Terry Harbour	MidAmerican Energy Company	1,3	MRO
					Tom Breene	Wisconsin Public Service	3,5,6	MRO
					Jeremy Volls	Basin Electric Power Coop	1	MRO
					Kevin Lyons	Central Iowa Power Cooperative	1	MRO
					Mike Morrow	Midcontinent Independent System Operator	2	MRO
Southwest Power Pool, Inc. (RTO)	Shannon Mickens	2	SPP RE	SPP Standards Review Group	Shannon Mickens	Southwest Power Pool Inc.	2	SPP RE
					Mike Buyce	City Utilities of Springfield	1,4	SPP RE
					Robert Gray	Board of Public Utilities,KS (BPU)	3	SPP RE
					Stewart Dover	Lafayette Utilities System	2	SPP RE

					John Allen	City Utilities of Springfield, Missouri	4	SPP RE
Public Service Enterprise Group	Sheranee Nedd	1,3,5,6	NPCC,RF	PSEG REs	Tim Kucey	PSEG - PSEG Fossil LLC	5	RF
					Karla Jara	PSEG Energy Resources and Trade LLC	6	RF
					Jeffrey Mueller	PSEG - Public Service Electric and Gas Co	3	RF
					Joseph Smith	PSEG - Public Service Electric and Gas Co	1	RF

1. The SDT asserts that the referenced data is already afforded protections at rest under existing CIP standards (CIP-003, 005, 007, etc.), is perishable, and has a diminished need for protection over time. Do you agree with the SDT's assertion? If you agree, please supply a rationale to support the position.

Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	No
Document Name	
Comment	
Texas RE requests the SDT consider defining the term "sensitive BES data", which could include ICCP, Historian, and backup data, since a goal of this project should be to provide clear requirements for identifying and protecting Control Centers required for reliable operation. The undefined term, sensitive BES data, is already being used among several non-CIP standards and defining the term would encourage consistency and lessen confusion.	
Likes 0	
Dislikes 0	
Response	

Aaron Austin - AEP - 3,5	
Answer	No
Document Name	
Comment	
AEP contends that CIP standards, specifically CIP-003,005,006, 007, 009, 010, and 011 concentrate on BCS, EACMS, PCA, PACS devices and data resident on them.	
Likes 0	
Dislikes 0	
Response	

Gerry Adamski - Essential Power, LLC - 5	
Answer	No
Document Name	
Comment	

Is the operational data a subset of all sensitive data? I would offer that certain modeling update information would not fall under this framework and could have negative impacts on the BES (e.g. ratings changes, configuration/outage changes, etc.). If that is captured in the scope of operational data, then ok but I infer from the presentation of the information that real-time variable data is what is being targeted here.

Likes 0	
Dislikes 0	

Response

Wendy Center - U.S. Bureau of Reclamation - 1,5

Answer	No
Document Name	

Comment

Reclamation recommends removing the phrase “is perishable, and has a diminished need for protection over time.” Reclamation agrees that data at rest is already afforded protections under other applicable CIP standards. Reclamation disagrees that all data at rest is perishable and has a diminished need for protection over time.

Likes 0	
Dislikes 0	

Response

Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6

Answer	No
Document Name	

Comment

AZPS agrees with the assumption that data at rest within a Control Center is already afforded protections under existing CIP standards (CIP-003-6, CIP-005-5, CIP-007-6, etc.), but respectfully notes that this assumption is outside the scope of the directive set forth by FERC in Order No. 822. Pursuant to FERC Order No. 822, Paragraph 53, the directive targets communication links and data **communicated between bulk electric system (“BES”) Control Centers.** (Emphasis Added.) Thus, the directive does not encompass or extend to include data at rest within BES Control Centers. Rather, it is intended to ensure that data in transit between such Control Centers are afforded appropriate protections. To ensure that the scope of the directive is accurately captured, AZPS offers the following revision to the referenced assumption:

Data at rest within a BES Cyber System is already afforded protections under existing CIP standards and is not within the scope of this directive.

Likes 0	

Dislikes 0	
Response	
Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Kinas - Orlando Utilities Commission - 3,5	
Answer	Yes
Document Name	
Comment	
Currently many PI or other Historians that store near real time data are located outside of ESPs since this data, once it is stored on the Historian is not used for operations. ***However some entities may use data stored on Histroians as a feedback loop into their control systems***. In these specific siturations the data "at rest" on the Historians may have an operational impact. Data that resides within an entities EMS is constantly being updated, the "data points" exist in memory and store data values in these data points are constantly being updated. If data wishes to be preserved it is written to a histroian before being overwirtten.	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	

Data needed for the operation of the BES is already protected and exists only to transmit operational controls which are transient in nature.

Likes 0	
Dislikes 0	

Response

Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF

Answer	Yes
Document Name	

Comment

The NSRF agrees with the SDT. NERC has already defined Operating Reliability Data (ORD) and recipients are required to sign an ORD Confidentiality Agreement, which should elimate the need for a requirement. Additionally, NERC Standards of Conduct as well as most FERC approved tariffs have provisions for protection of sensitive data.

Likes 0	
Dislikes 0	

Response

Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC

Answer	Yes
Document Name	

Comment

SRP agrees with the SDT assertions:

- CIP-003: Identifies all security management controls used by the entity to address high, medium, and low impact BES Cyber Systems (BCS).
- CIP-004: R4 Part 4.1 requires entities to develop processes to control not only electronic and physical access, it also requires processes to control access to designated BES Cyber System Information storage, otherwise known as repositories, as determined in CIP-011. These repositories are where “referenced data” would exist “at rest”.
- CIP-005: The entirety of the Standard is based on specifying a controlled Electronic Security Perimeter (ESP) in supporting of protecting BCS (including information “at rest” within the BCS).

- CIP-006: In the same manner as CIP-005 and ESP protections, the physical protections afforded by CIP-006 protect the BCS from unauthorized individuals “walking-up” to components of the BCS where “at rest” “referenced data” may exist.
- CIP-007: The entirety of the Standard is based on specifying technical, operational, and procedural controls to protect the BCS (including the information “at rest” within the BCS).
- CIP-010: The change and configuration management controls prevent and detect unauthorized changes to the BCS (including information “at rest” within the BCS). Vulnerability assessment requirements are also in support of protecting the BCS (including information “at rest” within the BCS).
- CIP-011: R1 requires the identification of BES Cyber System Information. An article of acceptable evidence included in the measures of R1 is the identification of “repositories or electronic and physical locations designated for housing BES Cyber System Information”. These identified locations are used as input for CIP-004 R4 Part 4.1 (in order to verify access controls).

Likes 0	
Dislikes 0	

Response

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority

Answer	Yes
Document Name	

Comment

The same information that is two seconds old in a real-time SCADA system may be retained for five years in a corporate (non-control) data historian. NERC CIP-002-5.1 scopes the applicability of the protections on assets which have a real-time impact on reliable BES operations. As such, any information utilized by real-time systems for a fifteen minute time horizon are already afforded protections in CIP-002 through 011.

While data at rest may have impacts on planning or historical analysis, it cannot be reasonably inferred to have a fifteen minute impact on reliable operations. Many multi-purpose Operating Systems support encrypted file systems. As such, any mandate for data at rest protections would be more appropriately scoped in CIP-011 and applied to electronic repositories of BES Cyber System information.

The Confidentiality, Integrity and Availability triad is commonly utilized in designing effective controls for information systems. Regulatory frameworks which provide protections for data at rest are focused on confidentiality of financial transactions and/or Personally Identifiable Information. Power control systems have unique characteristics which make Availability and Integrity paramount.

Encryption for data at rest inherently is focused on making access to information more restricted. This inherently creates potential to adversely impact Availability, which may be counter-productive to reliable BES operations.

Likes 0	
Dislikes 0	

Response

Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	Yes
Document Name	
Comment	
Supporting APPA comments	
Likes 0	
Dislikes 0	
Response	
Kelly Silver - Con Ed - Consolidated Edison Co. of New York - 1,3,5,6, Group Name Con Edison	
Answer	Yes
Document Name	
Comment	
We agree that existing CIP standards protections address the referenced data at rest. The referenced data is covered in the cited Standards. Consider that real-time SCADA data performance may be impacted by disk encryption.	
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 agrees with the assertion that the referenced data is already afforded protections under existing CIP standards.	
Likes 0	

Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8 - WECC	
Answer	Yes
Document Name	
Comment	
The data is resting on systems that are protected by CIP controls.	
Likes 0	
Dislikes 0	
Response	
Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
NRG agrees with the rationale because, the data at rest is not being used in the real-time operation of the Bulk Electric System i.e. the 15 minute impact process. Also, the CIP Standards provide the appropriate protection for data integrity and confidentiality for in-scope systems.	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	

The referenced data while at rest is covered in the cited Standards. Consider that real-time SCADA data performance may be impacted by disk encryption.	
Likes 1	Illinois Municipal Electric Agency, 4, Thomas Bob
Dislikes 0	
Response	
Jason Snodgrass - Georgia Transmission Corporation - 1	
Answer	Yes
Document Name	
Comment	
Once referenced data has been received by a BES Cyber Asset it is then protected under the CIP Standards. There is no need to protect stale data.	
Likes 0	
Dislikes 0	
Response	
Guy Andrews - Georgia System Operations Corporation - 3,4	
Answer	Yes
Document Name	
Comment	
Once referenced data has been received by a BES Cyber Asset it is then protected under the CIP Standards. There is no need to protect stale data.	
Likes 0	
Dislikes 0	
Response	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	

Comment	
ERCOT agrees with the SDT's assertion. ***While at rest***, the data required for reliable operation resides within existing BCS data and is afforded protections under existing CIP Standards. Much of the referenced data has a limited time of need for protection and can be made public after a certain number of days. Requiring additional protections of data at rest may not be necessary and due to the limited time of sensitivity, may not have a positive cost benefit.	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
In use and transport is the highest risk. Exisiting controls are sufficient.	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
BPA agrees with the SDT assertion. BPA believes the referenced data is already afforded protections at rest under existing standards.	
Likes 0	
Dislikes 0	

Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE	
Answer	Yes
Document Name	
Comment	
Xcel Energy agrees with the rationale that the data is perishable and is already afforded protection under existing CIP standards. Any data that is at rest does not meet the 15-minute impact criteria for adversely impacting real-time operations.	
Likes 0	
Dislikes 0	
Response	
Candace Morakinyo - WEC Energy Group, Inc. - 3,4,5 - MRO,RF	
Answer	Yes
Document Name	
Comment	
Existing CIP-011 requirements adequately identify and protect BES Cyber System information at rest.	
Likes 0	
Dislikes 0	
Response	
Deborah VanDeventer - Edison International - Southern California Edison Company - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Access to the host systems is strictly controlled via the current CIP standards and requirements.	
Likes 0	

Dislikes 0	
Response	
Mike Kraft - Basin Electric Power Cooperative - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Basin Electric Power Cooperative agrees NERC has already defined Operating Reliability Data and recipients are required to sign a Confidentiality Agreement, which should elimate the need for a requirement. In addition, Basin Electric agrees existing CIP standards provide protection for this data at rest.	
Likes 0	
Dislikes 0	
Response	
Brandon Cain - Southern Company - Southern Company Services, Inc. - NA - Not Applicable - SERC	
Answer	Yes
Document Name	
Comment	
Yes, Southern Company agrees with the SDT's assertion. Real-time reliability data used by Control Centers is only sensitive within a short time window; it becomes perishable quickly and the need to maintain protections for that data diminishes over time. For data "at rest", Southern Company views the language in the FERC Order, specifically paragraph 54, intending to address a reliability gap to protect communications between Controls Centers from "data manipulation type attacks" and "eavesdropping attacks". The existing controls applied in accordance with CIP-011 and CIP-006-6 R1.10 sufficiently address protection of sensitive BES data "at rest" and in logical transit within an ESP, respectively. Additionally, the existing controls applied in accordance with CIP-004 (Access Management), CIP-005 (ESPs, encryption, multi-factor authentication), and CIP-007 (system security controls, account management) provide by extension added layers of security to protect data "at rest."	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1,3,5,6	
Answer	Yes

Document Name	COMM Network - Exelon Comments - 3.13.17.docx
Comment	
See attachment Q1	
Likes 0	
Dislikes 0	
Response	
Mark Riley - Associated Electric Cooperative, Inc. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
AECI agrees that the referenced data is already afforded protections at rest under the current CIP Standards. Operational Reliability Data becomes stale over time and has a diminished need for protection.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion	
Answer	Yes
Document Name	
Comment	
The referenced data is covered in the cited Standards. Consider that real-time SCADA data performance may be impacted by disk encryption.	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	

Answer	Yes
Document Name	
Comment	
The SPP Standards Review Group agrees with the rationale because, the data at rest is not being used in the Real-time operation of the Bulk Electric System i.e. the 15 minute impact process. Also, the CIP Standards provide the appropriate protection for data integrity and confidentiality for in scope systems.	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	Yes
Document Name	
Comment	
Yes, much of the critical data between control centers is only valid for that immediate time period, control data hours or days old only has historical value.	
Likes 0	
Dislikes 0	
Response	
Charles Yeung - Southwest Power Pool, Inc. (RTO) - 2	
Answer	Yes
Document Name	
Comment	
• NERC has already defined Operating Reliability Data (ORD). Additionally, recipients are required to sign an ORD Confidentiality Agreement, which should elimate the need for a requirement.	
Likes 0	
Dislikes 0	

Response	
Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	
Tacoma supports the comments of Utility Services, Inc	
Likes 0	
Dislikes 0	
Response	
Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Glen Farmer - Avista - Avista Corporation - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrew Gallo - Austin Energy - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Preston Walker - PJM Interconnection, L.L.C. - 2 - SERC,RF	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lauren Price - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sheranee Nedd - Public Service Enterprise Group - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	

Likes 3	PSEG - Public Service Electric and Gas Co., 1, Smith Joseph; PSEG - PSEG Fossil LLC, 5, Kucey Tim; PSEG - Public Service Electric and Gas Co., 3, Mueller Jeffrey
Dislikes 0	
Response	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	Yes
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	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

2. If you do not agree with the SDT's assertion in Question 1, please identify the type of data, the risk posed at rest, and supply the rationale to support the position.

Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6

Answer	
Document Name	

Comment

No comment

Likes 0	
Dislikes 0	

Response

Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6

Answer	
Document Name	

Comment

AZPS respectfully asserts that the SDT's assertion in Question 1 is beyond the scope of the directive set forth in Order 822 at paragraph 53. Further, AZPS is concerned that the assumption paints all data retained with BES Control Centers with too "broad of a brush stroke." This is particularly evident in the SDT's assumption that all data within Control Centers is perishable and has a diminished need for protection as such statements appear to be considering the "freshness" of real-time data only.

AZPS notes that the data contained and retained within BES Control Centers includes more than real-time data. In particular, BES Control Centers often also retain data related to the operations and long-term planning time horizons. Such data, which is outside of data indicative of real-time status, may not age and become perishable in the same manner or time period as data communicating real-time status. Because the verbiage utilized in the assumption is extremely broad and does not clearly distinguish the or otherwise narrow the specific data to which the assumption applies, AZPS disagrees with the assumption set forth by the SDT as such assumption has the effect of "broad brushing" all data communicated between and "at rest" within BES Control Centers with the same importance and usability when, in fact, such data has varying levels of criticality, usability, confidentiality, etc.

AZPS reiterates that it agrees with the SDT that the risk associated with data "at rest" within Control Centers is negligible given the applicability of existing CIP reliability standards to such data, but, for the reasons set forth above, must respectfully disagree with the assumption and re-urge the SDT to adopt the proposed revisions recommended in response to Question 1.

Likes 0	
Dislikes 0	

Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE	
Answer	
Document Name	
Comment	
Not Applicable	
Likes 0	
Dislikes 0	
Response	
Candace Morakinyo - WEC Energy Group, Inc. - 3,4,5 - MRO,RF	
Answer	
Document Name	
Comment	
n/a	
Likes 0	
Dislikes 0	
Response	
Brandon Cain - Southern Company - Southern Company Services, Inc. - NA - Not Applicable - SERC	
Answer	
Document Name	
Comment	
N/A	
Likes 0	

Dislikes 0	
Response	
Chris Scanlon - Exelon - 1,3,5,6	
Answer	
Document Name	
Comment	
See attachment Q1	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 1,5	
Answer	
Document Name	
Comment	
Reclamation recommends removing the phrase “is perishable, and has a diminished need for protection over time.” Reclamation agrees that data at rest is already afforded protections under other applicable CIP standards. Reclamation disagrees that data all at rest is perishable and has a diminished need for protection over time. Reclamation recommends that each entity be responsible to determine the value of its data at rest, if and when the data at rest is perishable, and the necessary level of protection. As examples, some data between control centers may include sensitive data such as configuration information of the network or relay protection systems. If the data that is transferred is deemed to be sensitive, then the associated data at rest may also be sensitive.	
Likes 0	
Dislikes 0	
Response	
Aaron Austin - AEP - 3,5	
Answer	
Document Name	

Comment	
The CIP standards do not necessarily apply to Cyber Assets that perform operating day ahead activities or other comparable functions that may be capable of impacting the BES beyond the 15 minute threshold.	
Likes 0	
Dislikes 0	
Response	
Sheranee Nedd - Public Service Enterprise Group - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	
Document Name	
Comment	
N/A	
Likes 3	PSEG - Public Service Electric and Gas Co., 1, Smith Joseph; PSEG - PSEG Fossil LLC, 5, Kucey Tim; PSEG - Public Service Electric and Gas Co., 3, Mueller Jeffrey
Dislikes 0	
Response	
Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC	
Answer	
Document Name	
Comment	
HQT’s understanding of the objectives behind the drafting of CIP-012 is to protect communication links and therefore sensitive bulk electric system data exchanged between bulk electric system Control Centers in a manner that is appropriately tailored to address the risks posed to the BES by the assets being protected (i.e., high, medium, or low impact). Why are the security objectives are silent regarding avaibility? Protection of data at rest is (currently) not part of the objectives of CIP-012. Furthermore, our understanding of the different CIPs is that it does not fully address the security objectives of confidentiality and integrity of data at rest. CIP-005 is about establishing enclaves to protect the cybet assets, CIP-007 about the protection of the Cybe assets, CIP-011 to prevent unauthorized access (Guidelines and Technical Basis mention confidentiality but not integrity).	

Furthermore, the princips of CIA (Confidentiality Integrity Avaibility) may be implied but they are not precise enough to ensure that the objectives are meet in the existing CIP standards (CIP-003, 005, 007, 011 etc.). The concepts of confidentiality are treated in a certain ways but the concepts of integrity are not explicit. The objectifs of CIP-012 could say ”Develop a security plan to ensure the confidentiality, integrity of data at rest and in-transit between Control Centers, both inter-entity and intra-entity”	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	
Document Name	
Comment	
NA	
Likes 0	
Dislikes 0	
Response	
Gerry Adamski - Essential Power, LLC - 5	
Answer	
Document Name	
Comment	
See above	
Likes 0	
Dislikes 0	
Response	
Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	

Answer	
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Please see Texas RE’s response to #1.	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	
Document Name	
Comment	
See comment above.	
Likes 0	
Dislikes 0	
Response	

Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	
Document Name	
Comment	
Supporting APPA comments	
Likes 0	
Dislikes 0	
Response	
Andrew Gallo - Austin Energy - 1,3,4,5,6	
Answer	
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	

Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8 - WECC	
Answer	
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	
Document Name	
Comment	
n/a	
Likes 0	
Dislikes 0	
Response	
Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF	
Answer	
Document Name	
Comment	
See comments for Question No. 1	
Likes 0	
Dislikes 0	

Response	
Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC	
Answer	
Document Name	
Comment	
SRP agrees with the SDT’s assertion in Question 1.	
Likes 0	
Dislikes 0	
Response	

3. Future enforceable Reliability Standards IRO-010-2 and TOP-003-3 identify "data required for reliable operation." For example, Requirement R1 of IRO-010-2 states:

R1. The Reliability Coordinator shall maintain a documented specification for the data necessary for it to perform its Operational Planning Analyses, Real -time monitoring, and

1.1. A list of data and information needed by the Reliability Coordinator to support its Operational Planning Analyses, Real time monitoring, and Realtime Assessments including non -BES dat

TOP-003-3 Requirements R1 & R2 also have similar requirements for BAs and TOPs.

Do you agree that outlining this approach for identifying "data required for reliable operation" in the Guidelines and Technical Basis is sufficient; consequently, an additional definition of "sensitive BES data" or a requirement to identify "sensitive BES data" is not necessary? If not, please explain.

Andrew Gallo - Austin Energy - 1,3,4,5,6	
Answer	No
Document Name	
Comment	
The SDT should refine references to make it clear IRO-010 and TOP-003 data is limited to only data transmitted between control centers, because data between field assets and the control center is not in-scope. Also, this should not be in the Guidelines and Technical Basis section of a Standard because it would not be enforceable.	
Likes 0	
Dislikes 0	
Response	

Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	
CenterPoint Energy believes the "data required for reliable operation" identified in TOP-003-3 and IRO-010-2 is too broad and goes beyond the scope of "sensitive bulk electric system data" that should be protected. For example, portions of the data requested in TOP-003-3 and IRO-010-2 could be non-BES data that may only serve a purpose under certain system configurations or conditions. Data specified as necessary for Operational Planning Analyses is based in large part on projections and forecasts which should not fall under the label of "sensitive bulk electric system data." For example, outages, Facility Ratings, equipment limitations, and Protection System degradation use data exchange capabilities (phone systems, email, web based	

portals, FTP exchange, RTU, etc.) which may go beyond 'communication links' between Control Centers and should remain flexible enough to allow for normal and abnormal Real-time system conditions and what Operating Plans are being implemented at that time.

CenterPoint Energy recommends that the drafting team narrow the scope to a subset of the data identified in TOP-003-3 and IRO-010-2. CenterPoint Energy also recommends the drafting team develop criteria in the requirement language for determining what "sensitive bulk electric system data" should be separate from the holistic list of data necessary for functions described in the latest revisions of TOP and IRO Standards. CenterPoint Energy does not believe referencing the TOP-003-3 and IRO-010-2 standards in the requirement language is necessary as this may become problematic in the future if the language in these standards changes or becomes obsolete.

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

Duke Energy does not agree that a definition of "sensitive BES data" is not necessary. The question above alludes to expectations for the RC/BA/TOP in IRO-010-2 and TOP-003-3, but the reference fails to point out how this would apply to other functions such as the GOP. It is not enough to refer to the RC/BA/TOP data requirements if the standard is also applicable to other functions unless the applicability of data required from the GO/GOP/TO/DP by the RC/BA/TOP is limited.

Likes 0	
Dislikes 0	

Response

Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

SRP agrees that IRO-010-2 is the correct standard to identify "sensitive BES data"; however, SRP believes R3 should be used to determine what an entity is actually sending to the RC, as opposed to R1 (what the RC is asking for). This benefits entities with fewer functional registrations by eliminating data sources that are not applicable to them.

SRP agrees that TOP-003-3 R1 and R2 can be used to identify "sensitive BES data".

TOP-003-3: SRP provides the same evidence for both R1 and R2:

- R1: Data necessary for Operational Planning, Real-time monitoring, and Real-time Assessments.
- R2: Data necessary for analysis functions and Real-time monitoring.

SRP would like to see examples that include sensitive BES data transmitted between primary and back-up Control Centers. SRP also requests clarification on requirements for entities that own their communications network and protection of data transferred within the same private network.

Likes 0	
Dislikes 0	

Response

Richard Kinas - Orlando Utilities Commission - 3,5

Answer	No
Document Name	

Comment

The data for Operational Planning Analysis does not address the data that is used to perform other required functions such as calculating ACE for a BA. Data Required for reliable operation should include Data used during the performance of any Reliability Related Task (RRT) as defined with the entities training program under requirement PER-005-2 R1.1

Likes 0	
Dislikes 0	

Response

Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF

Answer	No
Document Name	

Comment

NRG suggests that the drafting team develop a definition for the term “sensitive BES data” - something similar in effect to the term “BES Cyber Systems Information” defined for CIP-011. Also, NRG recommends the definition for the term “sensitive BES data” include language addressing the 15 minute impact operational criteria.

NRG’s proposed language for “sensitive BES data” definition: “Data if rendered unavailable, degraded, or misused within 15 minutes would adversely impact the Real-Time operation of the Bulk Electric System.”

Our interpretation of the proposed language is that the drafting team has a concern for the protection of the data being transmitted. Since the data being transmitted can't be broken down and identified as sensitive data or non-sensitive data, the recommendation of developing a definition seems to be the safest path. Additionally, NRG recommends that the drafting team review the term "reliable operation" in the NERC Glossary of Terms. Also, if the term is used in the Requirement, NRG recommends using the term's definition out of the glossary. This is a defined term and we propose that the term should be capitalized. NRG seeks to understand, with this being a defined term, does this change the drafting team's intent for the use of this term?	
Likes 0	
Dislikes 0	
Response	
Jason Snodgrass - Georgia Transmission Corporation - 1	
Answer	No
Document Name	
Comment	
TOP-03-3 R1.1 requires a list of data and information needed, including non-BES data and external network data deemed necessary by the Transmission Operator. Because the requirement is vague using the verbiage such as "information needed" and "non-BES data" it may be difficult or impractical to protect the various methods used to communicate information or non-BES data. Methods of communication could include voice, email, text messages, or faxes.	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	No
Document Name	
Comment	
Responsible Entities are audited to the requirement language and cannot be held to the language in the GTB. If there is a desired outcome from a requirement, it should be stated in the requirement language; the GTB should not be used to imply the inherent meaning of a requirement. If the SDT's intent is to rely on documentation developed in TOP-003, the requirement should state that. If the SDT's intent is to rely on "a list of data and information needed by the Reliability Coordinator to support Operational Planning Analyses," etc., the requirement should state that. The GTB should provide only additional guidance.	
Likes 0	

Dislikes 0	
Response	
Aaron Austin - AEP - 3,5	
Answer	No
Document Name	
Comment	
AEP believes trying to connect multiple requirements to dissimiliar standards or standard families poses a huge risk in that altering the “origin” standard requirement without also modifying the “destination” requirement may result in a violation.Written guidelines provided by NERC explaining what “sesntive BES data” means would be helpful since the terms can be interpreted in various ways by each RC, BA and TOP.	
Likes 0	
Dislikes 0	
Response	
Guy Andrews - Georgia System Operations Corporation - 3,4	
Answer	No
Document Name	
Comment	
TOP-03-3 R1.1 requires a list of data and information needed, including non-BES data and external network data deemed necessary by the Transmission Operator. Because the requirement is vague using the verbiage such as “information needed” and “non-BES data” it may be difficult or impractical to protect the various methods used to communicate information or non-BES data. Methods of communication could include voice, email, text messages, or faxes.	
Likes 0	
Dislikes 0	
Response	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	

Comment
ERCOT does not agree with the approach of putting this in the Guidelines and Technical Basis section of a Standard since it is not enforceable or recognized by some ERO compliance staff. While the scoping of IRO-010 and TOP-003 may be too broad, having clear criteria will assist in clear implementation and understanding among the entities required to comply with the requirement. Without clear scope being defined, it could be left up to each responsile entity to determine what they think meets this criteria. That seems to be problematic since the responsible entities on each end of the communication link may not agree. It will also cause consistency issues with responsible entities that are under different regions. There will be a constant comparison of practices and could result in auditors determining what is necessary. The SDT should consider refining references to make it clear that IRO-010 and TOP-003 data is limited to only data transmitted between control centers. The data between field assets and the control center is out of scope. Also consider clarifying language that is clear that IRO-010 and TOP-003 informaton that is transferred verbally, including any VoIP, is not included in scope. In lieu of using IRO-010 and TOP-003, the SDT could consider creating a definition of the relevant data. Either of these approaches would be beneficial to facilitate getting necessary understanding, agreements, and/or regional rules implemented. Not having clear criteria will only increase the time needed to implement the standard. Entities will have to negotiate agreement on relevant data and then proceed with implementing protections.

Likes 0	
Dislikes 0	

Response

Gerry Adamski - Essential Power, LLC - 5	
Answer	No
Document Name	

Comment
If it inlcudes system configuration and modeling data that can be modified via inter-entity communication networks, then yes.

Likes 0	
Dislikes 0	

Response

Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE

Answer	No
Document Name	
Comment	

Many of the systems that are identified in the lists required by TOP-003 R1 and IRO-010 R1 are used for Operational Planning activities only and would not fully define what should fall within the 15 minute adverse impact criteria defined in current NERC CIP Standards which state that only systems that *if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System*.

Xcel Energy does not believe that IRO-010-2 and TOP-003-3 language adequately defines what 'sensitive data' should be included under this new Standard and that a definition of Sensitive Data needs to be created independent of TOP-003-3 requirements or any other Ops & Planning standard.

Likes 0	
Dislikes 0	
Response	

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group

Answer	No
Document Name	
Comment	

The SPP Standards Review Group suggests that the drafting team develops a definition for the term "sensitive BES data" something similar to the term "BES Cyber Systems Information" defined for CIP-011. Also, we recommend the definition for the term "sensitive BES data" include language addressing the 15 minute impact operational criteria.

SPP's proposed language for "sensitive BES data"definition:

Data if rendered unavailable, degraded, or misused within 15 minutes would adversely impact the Real-Time operation of the Bulk Electric System.

Our interpretation of the proposed language is that the drafting team has a concern for the protection of the data being transmitted. Since the data being transmitted can't be broken down and identified as sensitive data or non-sensitive data, the recommendation of developing a definition seems to be the safest path. Additionally, we recommend that the drafting team review the term "reliable operation" in the NERC Glossary of Terms. Also, if the term is used in the Requirement, we recommend using the term's definition out of the glossary. Our research shows that this is a defined term and we propose that the term should be capitalized. Finally, we would ask with this being a defined term, does this change the drafting team's intent for the use of this term?

Likes 0	
Dislikes 0	
Response	

Wendy Center - U.S. Bureau of Reclamation - 1,5	
Answer	No
Document Name	
Comment	
To promote consistency as the standards change, Reclamation recommends NERC define “sensitive BES data” and “data required for reliable operation” in the NERC Glossary of Terms so that these phrases may be used for all standards (specifically IRO, TOP, and CIP).	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1,3,5,6	
Answer	No
Document Name	
Comment	
See attachment Q1	
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 case can be made that a requirement to identify, or a definition of, “sensitive BES data” Is not necessary as it is already identified. In consideration of Question 3, we ask another question. The CIP Standards exist to address security risks of the BES to ensure reliability. In order to do that we protect the systems and infrastructure needed to perform the tasks or functions required for BES reliability operating services. Those systems predominately include the data necessary for these functions. “Are the CIP Standards meant to secure more than the data necessary to	

perform reliability tasks? And what gaps, if any, are not addressed or clearly identified in the data deemed necessary to perform reliability obligations in IRO-010-2?"

To protect BES reliability, entities are required under the CIP Standards to protect operational data and BES Cyber Systems Information. This is the same data identified as Real-time monitoring and Real-time Assessment data in IRO-010-2 R1 and TOP-003-3 R1 and R2. Thus the protections may need to be extended to consider Operational Planning Analysis or those data elements that are relevant to promulgate an attack with a longer shelf life of applicability or use.

Likes 0	
Dislikes 0	

Response

Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6

Answer	No
Document Name	

Comment

AZPS disagrees with the SDT's interpretation and asserions relative to broad applicability of the data required for reliable operation under TOP-003-3 and IRO-010-2 to the data contemplated in the directive set forth in Order 822 at paragraph 53. AZPS notes that both TOP-003-3 and IRO-010-2 and the data associated therewith are applicable to the operations planning time horizon and not the real-time operations time horizon. Given the focus of the FERC directive on data in transit between Control Centers during real-time operations, AZPS recommends that the SDT re-evaluate its interpretation as set forth above and assess the need for development of a definition of "sensitive BES data." To scope such definition, AZPS recommends that the SDT reference the definition of Real-Time Assessment in the Glossary of Terms, and those reliability standards that address the performance of Real-Time Assessments and monitoring to identify the data communicated between Control Centers in real-time for performance of such assessments and monitoring.

Further, since each entity has discretion to determine the confidential nature of its data, without a definition, different data could be assigned different levels of sensitivity and confidentiality by different entities. This would create unnecessary ambiguity and complexity for receiving entities – especially where such entity has multiple adjacent Balancing Authorities, Transmission Operators, Generation Operators, etc. AZPS respectfully asserts that, to eliminate inconsistencies and ensure that the real-time data that is critical to reliable operations is uniformly identified and protected amongst all interconnected entities, a definition is necessary.

Finally, AZPS notes that the Guidelines and Technical Basis is not enforceable in finding an entity out of compliance and should be available for supplemental information only. Therefore, while AZPS is not opposed to the provision of guidance, development of a definition for sensitive BES data to be included in the Glossary of Terms is recommended.

Likes 0	
Dislikes 0	

Response

Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	Yes
Document Name	
Comment	
Supporting APPA comments	
Likes 0	
Dislikes 0	
Response	
Preston Walker - PJM Interconnection, L.L.C. - 2 - SERC,RF	
Answer	Yes
Document Name	
Comment	
While PJM does agree with the draft language, we feel that it could be tied closely to the CIP-002 assessment (<15 minute impact). For entities that look to the guidance section and chose to use the IRO and TOP standards as a starting point, it should be more apparent that only data used for real-time reliability purposes, that fall within the 15 minute impact, would need to be protected per this standard. It could be mis-interpreted that the guidance suggests protecting all data included in the IRO and TOP standards, even data that may not fall into this real-time category.	
Likes 0	
Dislikes 0	
Response	
Kelly Silver - Con Ed - Consolidated Edison Co. of New York - 1,3,5,6, Group Name Con Edison	
Answer	Yes
Document Name	
Comment	
We agree using TOP-003 and IRO-010 Standards to identify data but we believe Operational Planning Analyses data is out of scope. Explicitly stating what data each entity requires in a Standard would not be beneficial. Currently each RC and TOP defines their own requirements for the data that they need from others (per TOP-003-3 and IRO-010). We are concerned that multiple definitions may lead to conflict.	

Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
We agree with the basic approach of using TOP-003 and IRO-010 Standards to identify this data but needs to be limited to real time data. We believe TOP-003 and IRO-010 include data that is not “real time” so would be outside this document’s scope. An example of data which is out of scope includes data used for Operational Planning Analyses.	
Likes 1	Illinois Municipal Electric Agency, 4, Thomas Bob
Dislikes 0	
Response	
Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC	
Answer	Yes
Document Name	
Comment	
HQT agree, but the reference should be clearly stated. Since IRO-010-2 and TOP-003-3 are future enforceable reliability Standards, the SDT should evaluate the risk of those not being endorsed. If this should happen, the basis would be absent of CIP-012. Also, with the present suggestion, CIP standard would be used to define controls of IRO and TOP standards. This situation could cause an audit gap: the CIP auditors would not have requirement from IRO or TOP to audit against and IRO and TOP auditors would not security requirement to audit against.	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	Yes

Document Name	
Comment	
SMUD does not recommend a prescriptive approach. It should be a risk based decision based on the entities risk anaysis.	
Likes 0	
Dislikes 0	
Response	
Candace Morakinyo - WEC Energy Group, Inc. - 3,4,5 - MRO,RF	
Answer	Yes
Document Name	
Comment	
The CIP standards are related to protecting BES Cyber Systems and BES Cyber System Information. The Ops and Planning standards are related to other aspects of reliabile operation. Any mixing and matching between CIP and non-CIP standards requirements is an opportunity for confusion, mistakes and potential compliance "double jeopardy".	
Likes 0	
Dislikes 0	
Response	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	Yes
Document Name	
Comment	
MMWEC supports comments submitted by APPA.	
Likes 0	
Dislikes 0	

Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion	
Answer	Yes
Document Name	
Comment	
We agree with the basic approach of using TOP-003 and IRO-010 Standards to identify this data but needs to be limited to real time data. We believe TOP-003 and IRO-010 include data that is not “real time” so would be outside this document’s scope. An example of data which is out of scope includes data used for Operational Planning Analyses.	
Likes 0	
Dislikes 0	
Response	
Brandon Cain - Southern Company - Southern Company Services, Inc. - NA - Not Applicable - SERC	
Answer	Yes
Document Name	
Comment	
Yes, Southern Company agrees with the SDT’s approach to utilizing existing Standard requirements that already require the identification of “data and information needed by the RC” to be referenced in the Guidelines and Technical Basis in forming the basis for data transmitted between Control Centers requiring protections in accordance with this Standard. Given the extensive amount of approved and enforceable Standard requirements, as well as those approved for future enforcement, filed with FERC, or under development that are addressing “data exchange via a secure network”, “all data between Control Centers to use a mutually agreeable security protocol”, and “procedures to address the quality of real-time data”, Southern Company agrees that the specific requirements of IRO-010 and TOP-003 sufficiently address the identification of data needing to be protected when transmitted between Control Centers. Any additional attempt to define “sensitive BES data” or to add additional requirements to identify “sensitive BES data” is not necessary.	
Likes 0	
Dislikes 0	
Response	
Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6	
Answer	Yes

Document Name	
Comment	
Tacoma supports the comments of Utility Services, Inc	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	Yes
Document Name	
Comment	
We do not need a clarifier.	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1,3,5,6	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Lauren Price - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sheranee Nedd - Public Service Enterprise Group - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	
Likes 3	PSEG - Public Service Electric and Gas Co., 1, Smith Joseph; PSEG - PSEG Fossil LLC, 5, Kucey Tim; PSEG - Public Service Electric and Gas Co., 3, Mueller Jeffrey
Dislikes 0	
Response	

Anton Vu - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Riley - Associated Electric Cooperative, Inc. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Kraft - Basin Electric Power Cooperative - 1,3,5,6	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Charles Yeung - Southwest Power Pool, Inc. (RTO) - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Please see Texas RE’s response to #1.	
Likes 0	
Dislikes 0	
Response	

4. The SDT asserts that "availability" of inter-and intra-entity Control Center communication of data is being addressed in Project 2016-01 Modifications to TOP and IRO Standards, specifically Reliability Standards TOP-001-4 and IRO-002-5. The proposed standards require redundant and diversely routed data exchange capabilities at a Responsible Entity's primary Control Center. Do you agree that "availability" is adequately addressed by these standards? If not, please provide rationale to support your position.

Wendy Center - U.S. Bureau of Reclamation - 1,5	
Answer	No
Document Name	

Comment

To promote consistency as the standards change, Reclamation recommends NERC define "availability" in the NERC Glossary of Terms so that the term may be used for all standards (specifically IRO, TOP, and CIP standards).

Likes 0	
Dislikes 0	

Response

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	

Comment

BPA does not agree that "availability" is adequately addressed by redundant and diversely routed data exchange capabilities at the primary Control Center for the following reasons:

1. Currently, the proposed language on page 2 includes protection of "confidentiality and integrity of data required for reliable operation of the BES" and eliminates "availability" from the language of the requirement. However, in the Confidentiality/Integrity/Availability (CIA) triad for information security, each leg must be balanced against the other two legs. By segregating Availability to TOP-001-4 and IRO-002-5, while leaving Confidentiality/Integrity in the proposed CIP-012 standard, it becomes impossible to properly balance all three legs of the triad to achieve optimum Reliability of the BES. The cyber security triad represents design tradeoffs; entities can't properly design communications networks – or worse: existing infrastructure may need to be rebuilt – if one of the options (Availability) is removed from consideration.

2. While the requirements of TOP-001-4 and IRO-002-5 (redundancy and diverse routing of data) can be used to achieve increased Availability, it can also be achieved through other equally effective methods. Therefore, "availability" is not adequately addressed by TOP-001-4 and IRO-002-5 and limits entities' options to address availability by other methods more appropriate to their systems.

Therefore, BPA proposes that "availability" be added into the proposed language on page 2 to meet the security objectives of Order 822, i.e., "…to protect AVAILBILITY, confidentiality and integrity of data required for reliable operation...."

BPA also encourages the SDT to use the Guidelines and Technical Basis section to recognize the distinction between the engineering/design term "availability" (in which availability is quantitative – e.g., a system is designed to be available 99.99% of the time) and the cyber security application in which availability is a qualitative element of security that is constantly balanced against two other (often competing) elements (confidentiality and integrity).

Likes 0	
Dislikes 0	

Response

Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	No
Document Name	

Comment

CenterPoint Energy does not believe that TOP-001-4 and IRO-002-5 adequately address availability of inter-entity and intra-entity Control Center communication of data. Both Standards speak to data exchange capability having redundant and diversely routed data exchange infrastructure (hardware) once external data enters the primary Control Center. TOP-001-4 and IRO-002-5 do not ensure availability or communication of data between inter-entity and intra-entity Control Centers, but only the redundancy of infrastructure internal to the requesting entity's primary Control Center. Rationale language is specific to this, "Infrastructure that is not within the TOP's primary Control Center is not addressed by the proposed requirement." CenterPoint Energy believes data exchange capability used in TOP-001-4 does not fully address 'data links' between inter-entity and intra-entity Control Centers.

CenterPoint Energy recommends the drafting team re-evaluate "availability" and how it can be adequately addressed by other existing standards.

Likes 0	
Dislikes 0	

Response

Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6

Answer	Yes
Document Name	

Comment

Tacoma supports the comments of Utility Services, Inc

Likes 0	

Dislikes 0	
Response	
Brandon Cain - Southern Company - Southern Company Services, Inc. - NA - Not Applicable - SERC	
Answer	Yes
Document Name	
Comment	
Yes, Southern Company agrees with the SDT that “availability” is adequately addressed by the other Standards referenced and by common industry practices. Southern Company also offers to the SDT that the only aspect of cyber security at issue under this directive is data integrity. Not only is it appropriate for this effort to be silent regarding availability, we would request that the SDT consider that this Standard should also remain silent regarding “confidentiality.” Including confidentiality will likely result in unintended consequences with no commensurate reduction in risk to BES reliability.	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
See attachment Q1	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion	
Answer	Yes
Document Name	
Comment	

Availability is adequately covered by other standards.	
Likes 0	
Dislikes 0	
Response	
Candace Morakinyo - WEC Energy Group, Inc. - 3,4,5 - MRO,RF	
Answer	Yes
Document Name	
Comment	
Redundancy and diversity are the primary tools available to support "availability".	
Likes 0	
Dislikes 0	
Response	
Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC	
Answer	Yes
Document Name	
Comment	
HQT agree, but the reference should be clearly stated. Since IRO-010-2 and TOP-003-3 are future enforceable reliability Standards, the SDT should evaluate the risk of those not being endorsed. If this should happen, the basis would be absent of CIP-012. Also, with the present suggestion, CIP standard would be used to define controls of IRO and TOP standards. This situation could cause an audit gap: the CIP auditors would not have requirement from IRO or TOP to audit against and IRO and TOP auditors would not security requirement to audit against.	
Likes 0	
Dislikes 0	
Response	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes

Document Name	
Comment	
ERCOT agrees with the SDT's assertion that "availability" is currently addressed by other reliability standards. While TOP-001-4 and IRO-002-5 do address availability, the SDT could cite more of the standards that provide this compliance and enforcement coverage.	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Availability is adequately covered by other standards.	
Likes 1	Illinois Municipal Electric Agency, 4, Thomas Bob
Dislikes 0	
Response	
Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
SRP has been generally supportive of the direction the SDT has gone for both TOP-001-4 and IRO-002-5 standard development under project 2016-01.	
Likes 0	
Dislikes 0	
Response	
Kelly Silver - Con Ed - Consolidated Edison Co. of New York - 1,3,5,6, Group Name Con Edison	

Answer	Yes
Document Name	
Comment	
Availability is already defined in the data specifications of each RC and TOP.	
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 agrees that the “availability” of this data is being addressed in Project 2016-01 Modifications to TOP and IRO Standards. We would like to mention to the drafting team that the definition of “Control Center” may need to be re-visited as a result of these new protections. Currently, the definition of “Control Center” may include generation control rooms. We do not believe that these additional protections being proposed by the draft language should be applicable to generation control rooms.	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	Yes
Document Name	
Comment	
Supporting APPA comments	
Likes 0	
Dislikes 0	
Response	

sean erickson - Western Area Power Administration - 1,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Charles Yeung - Southwest Power Pool, Inc. (RTO) - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes
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	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Kraft - Basin Electric Power Cooperative - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Riley - Associated Electric Cooperative, Inc. - 1,3,5,6	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Gerry Adamski - Essential Power, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sheranee Nedd - Public Service Enterprise Group - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	
Likes 3	PSEG - Public Service Electric and Gas Co., 1, Smith Joseph; PSEG - PSEG Fossil LLC, 5, Kucey Tim; PSEG - Public Service Electric and Gas Co., 3, Mueller Jeffrey
Dislikes 0	

Response	
Guy Andrews - Georgia System Operations Corporation - 3,4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Austin - AEP - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jason Snodgrass - Georgia Transmission Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lauren Price - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Kinas - Orlando Utilities Commission - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Preston Walker - PJM Interconnection, L.L.C. - 2 - SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Andrew Gallo - Austin Energy - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE does not have comments in response to this question.	
Likes 0	
Dislikes 0	
Response	

5. The SDT is proposing to develop a new CIP standard because the directives of FERC Order 822 related to the protection of communication networks used to exchange sensitive BES data regardless of the entity's size or impact level. Do you agree with the drafting of a new CIP standard to address this issue? If you disagree and would prefer to include requirements in existing CIP Standards, such as CIP-003 and CIP-005, please provide rationale and propose requirement language.

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority

Answer	No
Document Name	

Comment

Any focus on protection of communications networks is misplaced. Protection of data, regardless of the communications medium or network, needs to be the focus of any standards development activities.

Distributed generation, proliferation of smart metering, and ever increasing capabilities in speed and bandwidth of communications technologies are creating new sources of data that can be beneficial in real-time power operations. Entities require innovative mechanisms to securely acquire real-time information into SCADA systems to enable better decision making, whether the data comes via cellular, satellite, leased line, or private carrier connections.

NERC should benchmark with other regulatory bodies which oversee industries with similar needs, such as the financial sector. The financial industry originally used carbon-paper copies of credit cards, submitted to centralized clearing houses, to process credit transactions. Visa provided the first electronic, real-time transaction clearing terminal in 1979. The technologically has proliferated to the point that any smart phone can be used to execute financial transactions in real time. The physical and cyber security of the end points themselves may not be under control of financial institutions. Essentially, what the financial sector has done is provide interfaces to a very sensitive network to millions of devices in real time.

There are many parallels to the power sector, wherein a large quantity of devices increasingly need to send data to control systems over a variety of communications technologies securely, in real-time.

Financial companies have an inherent financial interest in maximizing availability and accessibility of the financial network to increase transactions. Power systems have an inherent reliability interest in getting more information to enable operators to make better real-time decisions.

NERC is in a unique position wherein it may leverage lessons learned from others industries who have decades of experience addressing these types of issues. Any standards development would greatly benefit from cross-pollinization of expertise and not be overly prescriptive so as to limit emerging technologies such a quantum or crypto block chain techniques.

Likes 0	
Dislikes 0	

Response

Preston Walker - PJM Interconnection, L.L.C. - 2 - SERC,RF

Answer	No
Document Name	

Comment
PJM would prefer to put the language in CIP-005 for Highs and Mediums and CIP-003 for Lows.

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
Duke Energy disagrees with the drafting of a new standard to address this directive. We feel that based on the current draft language, this requirement would be better suited in CIP-003-3. Adding to an already existing framework rather than creating a new standard is preferable. Creating a new standard would also require an entity to create additional documentation, rather than adding to already existing documentation.

Likes 0	
Dislikes 0	

Response

Kelly Silver - Con Ed - Consolidated Edison Co. of New York - 1,3,5,6, Group Name Con Edison

Answer	No
Document Name	

Comment
We believe that protection of communications networks would best be incorporated into existing CIP-005 or CIP-011 Standards.

Likes 0	
Dislikes 0	

Response

Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC

Answer	No
Document Name	
Comment	

SRP disagrees with the proposition to develop a new CIP standard. SRP suggests keeping requirements for low impact systems in CIP-003. Since CIP-005 already protects the BCS up to the point of EAP, it is possible to add another requirement to protect “BES sensitive data” between EAPs via site to site encryption, application layer encryption, or physical protections (as described in the “Draft Guidance” section). In addition to CIP-003 and CIP-005, the SDT should consider modifying CIP-006 R1.10, which includes requirements to protect cabling and other nonprogrammable communication components, to ensure no conflicts.

SRP prefers a risk-based approach that has different requirements for high, medium, and low impact systems.

Likes 0	
Dislikes 0	
Response	

Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF

Answer	No
Document Name	
Comment	

If the objective is to provide protection of the telecommunications interface or boundaries at control centers, it appears this is already addressed under CIP-002 and CIP-006. Clarifying language for existing standards would be sufficient to address protection issues.

Likes 0	
Dislikes 0	
Response	

Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric

Answer	No
Document Name	
Comment	

The existing cyber security controls in CIP-003 and CIP-005 already provide the basis for the protection of the communication links between control centers. It is better to enhance these requriements to include the communication links then a new requirement

Likes 0	
Dislikes 0	
Response	
Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	No
Document Name	
Comment	
NRG recommends maintaining the current Standards (CIP-003, CIP-005, CIP-006, CIP-007, and CIP-011) and revise them accordingly or as needed to protect the data. These particular Standards have the potential to address the concerns pertaining to sensitive BES data, regardless of the entity's size or impact level. Also, they can reduce the potential of creating redundancy issues.	
Likes 0	
Dislikes 0	
Response	
Jason Snodgrass - Georgia Transmission Corporation - 1	
Answer	No
Document Name	
Comment	
If the SDT develops a new CIP standard it could be difficult for an entity to know which standard to apply if there is any overlap between existing standards and thus the preference would be to incorporate any new requirements into CIP-003 and CIP-005.	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	No
Document Name	
Comment	

In isolation, it might be less confusing to group the new requirements together; however, the continued addition of new standards, attachments, etc. has made the standards increasingly difficult for Responsible Entities to fully understand and comply with. If these new requirements are necessary, IPC suggests adding them to CIP-005-5 as R3 with associated parts since CIP-005-5 deals with ESP boundaries and external connections.

Likes 0	
Dislikes 0	

Response

Aaron Austin - AEP - 3,5

Answer	No
Document Name	

Comment

Requirements for communications to high and medium impact BCS should reside in the location with the other electronic access requirements in CIP-005. Similarly, the requirements for communications between low impact BCS at control centers should reside with the other requirements for low impact BCS written comenserate with the risk. There should be a “high water mark” provision to protect communications from low impact BCS at control centers to high and/or medium impact BCS at control centers.

Likes 0	
Dislikes 0	

Response

Guy Andrews - Georgia System Operations Corporation - 3,4

Answer	No
Document Name	

Comment

If the SDT develops a new CIP standard it could be difficult for an entity to know which standard to apply if there is any overlap between existing standards and thus the preference would be to incorporate any new requirements into CIP-003 and CIP-005.

Likes 0	
Dislikes 0	

Response

Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC	
Answer	No
Document Name	
Comment	
CIP-005 is used to define the network compliance controls. Spreading network compliance controls throughout different CIP could result in confusion in the application of the different required controls. The CIA requirements for data (in transit or at rest) should be explicitly defined in CIP-005.	
Likes 0	
Dislikes 0	
Response	

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	

BPA does not agree that a new standard is required. A new standard could result in isolated requirements that do not blend with – or even contradict – existing requirements. The objectives can be met by coordinating with existing standards such as CIP-003 & CIP-005.

BPA also proposes that the Guidelines and Technical Basis section should emphasize that entities can/should leverage evidence from the numerous other CIP standards where data quality, confidentiality and availability is also addressed.

Potential language to be incorporated into CIP-005-x R3:

Applicable Systems: High Impact BES Cyber Systems at Control Centers; Medium Impact BES Cyber Systems at Control Centers

Requirements: R3. The Responsible Entity shall implement one or more documented plan(s) that achieve the security objective to protect availability, confidentiality and integrity of data required for reliable operation of the BES. The plan applies to data being transferred across communication networks between Control Centers, both inter-entity and intra-entity and shall include each of the applicable requirement parts in CIP-005-x Table R3.

3.1 Identify data required for reliable operation of the BES (if not already identified under IRO-010-2 and TOP-003-3).

3.2 Where technically feasible, have one or more methods for protecting availability, confidentiality and integrity of the data identified in 3.1.

3.3 Have one or more methods for alarming to a central location when loss of protection of data failed to a central location with a method of immediate response.

3.4 Have one or more methods for timely response to alarms identified in 3.3.

Potential language to be incorporated into the next version of CIP-003-x, R1.2, For its assets identified in CIP-002 containing low impact BES Cyber Systems, if any: *New:* 1.2.7. Ensuring the availability, confidentiality and integrity of data required for reliable operation of the BES between Control Centers, both inter-entity and intra-entity.	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	No
Document Name	
Comment	
No – utilize existing standards. The impact level should be considered within the the context of existing standards.	
Likes 0	
Dislikes 0	
Response	
Candace Morakinyo - WEC Energy Group, Inc. - 3,4,5 - MRO,RF	
Answer	No
Document Name	
Comment	
It may be impossible to protect the "networks". It is more important to ensure the availability, confidentiality and integrity of the data flowing over those networks. As previously noted, redundancy and diversity, along with monitoring, are tools which can ensure availability, and can be addressed in the ops & planing standards. Properly implemented encryption, is a tool which can ensure confidentiality and integrity of the data and can be addressed within CIP-005.	
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 believes a new Standard is not required to address the risks identified in FERC Order 822. Xcel Energy believes that existing CIP-003 and CIP-005 standards should be updated as determined necessary to address the concerns identified in the order. Current CIP Standards include a comprehensive set of requirements to protect the Bulk Electric System and specific controls to address new risks should be integrated into existing requirements when possible. Creating a new standard would add unnecessary complexity and lead to confusion when it may include requirements already covered by CIP-003, CIP-005, CIP-006 and potentially CIP-011. The development of a new Standard to address this concern without coordination of existing CIP requirements would also create an unknown and complex audit approach with risk of creating instances of double jeaproady that could otherwise be prevented with proper integration and revisions of current CIP Standards to address the concern.	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	No
Document Name	
Comment	
We recommend maintaining the current Standards (CIP-003, CIP-005) and revising them accordingly or as needed. These particular Standards have the potential to address the concerns pertaining to sensitive BES data regardless of the entity's size or impact level. Also, they can reduce the potential of creating redundancy issues.	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 1,5	
Answer	No
Document Name	
Comment	

Reclamation recommends the requirements for protecting communication networks should be included in CIP-003-7i for low impact BES Cyber Systems; and CIP-005-5 for the high and medium BES Cyber Systems.

Likes 0	
Dislikes 0	

Response

Brandon Cain - Southern Company - Southern Company Services, Inc. - NA - Not Applicable - SERC

Answer	No
Document Name	

Comment

Southern Company disagrees with this approach and respectfully requests the SDT to consider the technical and procedural controls that result from these new requirements will almost certainly be designed, implemented, and maintained in conjunction with the controls in CIP-005 (for Highs and Mediums) and CIP-003 (for Lows). Rather than create a new set of requirements, guidance, RSAWs, etc. for something that will have to be audited along with and as if it were a part of CIP-005 (for Highs and Mediums) or part of CIP-003 (for Lows), we would recommend modifying those Standards.

Likes 0	
Dislikes 0	

Response

Mike Kraft - Basin Electric Power Cooperative - 1,3,5,6

Answer	No
Document Name	

Comment

Basin Electric would prefer low impact requirements be kept in CIP-003 as this minimizes potential confusion with low impact level only entities. Basin Electric would prefer additions to CIP-005 vs. a new standard as the protections for high and medium impact levels would be closely tied to an Electronic Security Perimeter and crossing the applicable boundary for a Control Center.

Likes 0	
Dislikes 0	

Response

Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	No
Document Name	
Comment	
AZPS can see the value in the development of an entirely new standard; however, AZPS is concerned that the development of an entirely new standard is beyond the scope of the FERC directive, which states that “modifications to CIP-006-6 to provide controls to protect, at a minimum, communication links and data communicated between bulk electric system Control Centers are necessary in light of the critical role Control Center communications play in maintaining bulk electric system reliability.” Therefore, AZPS requests that the SDT evaluate and clarify whether the SAR provides the additional authority necessary for the development of a new standard, as opposed to the modification of CIP-006-6.	
Likes 0	
Dislikes 0	
Response	

Charles Yeung - Southwest Power Pool, Inc. (RTO) - 2	
Answer	No
Document Name	
Comment	
If the objective is to provide protection of the telecommunications interface or boundaries at control centers, it appears this is already addressed under CIP-002 and CIP-006. At most this would require some clarifying language.	
Likes 0	
Dislikes 0	
Response	

sean erickson - Western Area Power Administration - 1,6	
Answer	No
Document Name	
Comment	

Per the NSRF: If the objective is to provide protection of the telecommunications interface or boundaries at control centers, it appears this is already addressed under CIP-002 and CIP-006. Clarifying language for existing standards would be sufficient to address protection issues.	
Likes 0	
Dislikes 0	
Response	
Andrew Gallo - Austin Energy - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	
A new standard will assist in defining the requirements addressing the inter-relationship between entities of differing impact levels.	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	Yes
Document Name	
Comment	
Supporting APPA comments	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes

Document Name	
Comment	
The Standard Drafting Team's proposed approach seems consistent with the discussion in FERC Order No. 822 delineating between the CIP Standards focusing on "boundary" issues – that is, the definition of boundaries and the creation of protections at those boundaries – and the data security and communication link issue for BES sensitive data being transmitted across such boundaries.	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
There are concerns about the applicability section and how it will interact with the existing CIP Standards exemption 4.2.3.2. The applicability section should limit the scope to only real time communication networks or data between Control Centers. Would like additional guidance on the applicability of technologies like voice communication email, text messaging … Consider including language for CIP Exceptional Circumstances	
Likes 1	Illinois Municipal Electric Agency, 4, Thomas Bob
Dislikes 0	
Response	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Since these requirements are not limited to just communications between entities at the same impact level, a new standard will assist in defining the requirements that address the interrelationship between entities of differing impact levels.	

Likes 0	
Dislikes 0	
Response	
Sheranee Nedd - Public Service Enterprise Group - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	
A new standard would be less disruptive. This way all policy/procedure changes would be contained in 1 document.	
Likes 3	PSEG - Public Service Electric and Gas Co., 1, Smith Joseph; PSEG - PSEG Fossil LLC, 5, Kucey Tim; PSEG - Public Service Electric and Gas Co., 3, Mueller Jeffrey
Dislikes 0	
Response	
Gerry Adamski - Essential Power, LLC - 5	
Answer	Yes
Document Name	
Comment	
A new standard would be preferred to specify the communication network requirements.	
Likes 0	
Dislikes 0	
Response	
Deborah VanDeventer - Edison International - Southern California Edison Company - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	

Because of the way SCE has organized the assignment of CIP requirements into Programs, this has no impact to us operationally. SCE believes the general benefit of creating a new CIP standard (CIP-012) is that like requirements would be grouped together and easier to locate.	
Likes 0	
Dislikes 0	
Response	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	Yes
Document Name	
Comment	
MMWEC supports comments submitted by APPA.	
Likes 0	
Dislikes 0	
Response	
Mark Riley - Associated Electric Cooperative, Inc. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
The requirements span multiple impact levels and a new standard would assist entities in identifying the applicability of the new requirements.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion	
Answer	Yes
Document Name	

Comment	
Request the SDT consider and address how existing CIP Standards exemption 4.2.3.2 could be impacted. There are concerns about the applicability section and how it will interact with the existing CIP Standards exemption 4.2.3.2. The applicability section should limit the scope to only real time communication networks or data between Control Centers. Would like additional guidance on the applicability of technologies like voice communication email, text messaging. Consider including language for CIP Exceptional Circumstances.	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
See attachment Q1	
Likes 0	
Dislikes 0	
Response	
Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	
Tacoma supports the comments of Utility Services, Inc	
Likes 0	
Dislikes 0	

Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lauren Price - American Transmission Company, LLC - 1	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	Yes
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	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	

6. The SDT evaluated multiple approaches to addressing the directive. The approach proposed in this informal posting focuses on the protection of communication links. An alternative approach could focus on the protection of the sensitive BES data itself. Do you agree with the SDT's approach to focus the draft language on the protection of communication links? If not, please provide rationale and propose alternative language.	
sean erickson - Western Area Power Administration - 1,6	
Answer	No
Document Name	
Comment	
What you are trying to protect data/link/network will ultimately determine how best to protect it, and it is not clear from this request what that is. per the NSRF: The NSRF recommends focusing on the boundaries or interface points, not the links between control centers.	
Likes 0	
Dislikes 0	
Response	
Charles Yeung - Southwest Power Pool, Inc. (RTO) - 2	
Answer	No
Document Name	
Comment	
We agree with focusing on the boundaries or interface points, not the links between control centers.	
Likes 0	
Dislikes 0	
Response	
Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6	
Answer	No
Document Name	
Comment	

Tacoma supports the comments of Utility Services, Inc	
Likes 0	
Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	No
Document Name	
Comment	
AZPS does not agree that protection of the communication links alone achieves the FERC directive, which also references controls to protect the data communicated between BES Control Centers. Controls that would be applicable to the protection of data include controls such as encryption, which is different and superior to the controls that would be used to protect communication links alone.	
Likes 0	
Dislikes 0	
Response	
Mike Kraft - Basin Electric Power Cooperative - 1,3,5,6	
Answer	No
Document Name	
Comment	
Basin Electric prefers objective based standards/requirements. If the objective can be met via multiple methods (e.g. protected communication links or protecting the data itself), Basin Electric would prefer the flexibility to choose the approach and method. The proposal does include flexibitily within the protection of communication links approach which is appreciated.	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 1,5	

Answer	No
Document Name	
Comment	
Reclamation recommends including requirements for protecting communication networks in CIP-003-7i for low impact BES Cyber Systems, in CIP-005-5 for high and medium BES Cyber Systems, and in CIP-006-6 Requirement R1 Part 1.10 for physical security.	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	No
Document Name	
Comment	
The review group recommends working on a multiple approach solution to address the directive. The Primary Solution could address the protection of the communication link. As an alternative method, we recommend the drafting team consider other methods that are not link level controls. Additionally, we would ask the drafting team to provide clarity on the difference between “communication links” and “communication networks”.	
Likes 0	
Dislikes 0	
Response	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	No
Document Name	
Comment	
MMWEC supports comments submitted by APPA.	
Likes 0	
Dislikes 0	
Response	

Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE	
Answer	No
Document Name	
Comment	
The SDT should continue to evaluate multiple approaches to address the directive. Allowing the entity to determine which is appropriate based on situation. It might not be feasible to always implement link controls between entities.	
Likes 0	
Dislikes 0	
Response	
Candace Morakinyo - WEC Energy Group, Inc. - 3,4,5 - MRO,RF	
Answer	No
Document Name	
Comment	
Rather than focusing on the links, we should focus on protecting the data. If that means implementing certain protections such as encryption over the links, that's fine. Don't focus on the links themselves.	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	No
Document Name	
Comment	
No – SMUD requests that the definition of communication links should be clarified.	

Likes 0	
Dislikes 0	

Response

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

BPA does not agree that focusing on protection of the communication links is the best approach to meet the FERC directive. Merely protecting the network, or communications links, does not necessarily protect the data carried by the network. However, if the requirement instead emphasizes protection of data, BPA believes entities will gain the additional benefit of creating a more secure cyber environment overall.

BPA proposes that draft language be revised to require method(s) for protecting “applicable data” rather than “communication links” between Control Centers.

Likes 0	
Dislikes 0	

Response

Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC

Answer	No
Document Name	

Comment

The strategy of protecting the sensitive BES data itself is a better one than to focus on wether the data is at rest or in-transit. The CIA objectives could be added to CIP-005 & CIP-011. This would maintain the current consistency and approach of the CIP standard.

Likes 0	
Dislikes 0	

Response

Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
ERCOT does not agree with protection of communication links. The requirement should be written to allow entities to implement the program that fits their needs and infrastructure. Some may be best suited to protect the data and others may be best suited in protecting the communication links. The security objects should remain as it is with options in how to achieve the objective as articulated in the draft guidance.	
Likes 0	
Dislikes 0	
Response	

Guy Andrews - Georgia System Operations Corporation - 3,4	
Answer	No
Document Name	
Comment	
Either of the two approaches could provide good security measure but why limit the entity to only one approach. It would be better to allow each entity to choose their own approach which best fits their environment.	
Likes 0	
Dislikes 0	
Response	

Aaron Austin - AEP - 3,5	
Answer	No
Document Name	
Comment	
AEP believes the security directive for the requirements should be written in a way to permit any responsible entity to achieve the directive, regardless of technology or preferred architecture.	
Likes 0	

Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	No
Document Name	
Comment	
Either approach of protecting the data or the communication links should be an option for a Responsible Entity as long as the Responsible Entity meets the security objective of providing confidential data that has integrity.	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	No
Document Name	
Comment	
We like the option to protect either the data or the links. We would like to see these options clearly defined within the requirements and not just in the guidance. The Standard should be an outcome based Standard. FERC Order 822 section 58 clarifies this scope as inter-Control Center and intra-Control Center communications. The guidance seems to extend the scope beyond this by including references to DP's and listing Data links without reference to Control Centers.	
Likes 1	Illinois Municipal Electric Agency, 4, Thomas Bob
Dislikes 0	
Response	
Jason Snodgrass - Georgia Transmission Corporation - 1	
Answer	No
Document Name	

Comment
Either of the two approaches could provide good security measure but why limit the entity to only one approach. It would be better to allow each entity to choose their own approach which best fits their environment.

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	No
Document Name	

Comment
Texas RE suggests that the suggested requirements could be more clear. FERC Order No. 822, P. 56 provides that "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." Elsewhere, FERC Order No. 822 specifically refuted reliance on the EOP-008-1 Standard because that Standard "does not provide for the protection of communication links and sensitive bulk electric system data communicated between bulk electric systems Control Centers." FERC Order No. 822, P. 63. In short, FERC Order No. 822 appears to specifically contemplate protections for both communications links and electric system data as separate categories. On page 4 of the Unofficial Comment Form, the Standard Drafting Team (SDT) notes that "the Responsible Entity must document and implement plans for the protection of the confidentiality and integrity of operational reliability data communicated between Control Centers." The SDT then references examples of methods to protect data, such as site to site encryption and application layer encryption. Texas RE believes these are appropriate examples of methods to protect electric system data that is consistent with the intent of FERC Order No. 822. However, Texas RE is concerned that the SDT's proposal potentially subsumes these data-focused protection methods under protections for physical communications links themselves. Although such protections are appropriate, FERC Order No. 822 appears to view data security and physical communications link protections as separate, augmentative elements of a robust data security program. As such, Texas RE recommends that the SDT further specify that in order to achieve the security objective to protect confidentiality and integrity of data required for the reliable operation of the BES, responsible entities include the following language: **1.4 Method(s) for protecting the operational reliability of data communicated between Control Centers identified in 1.1, where technically feasible.**

Likes 0	

Dislikes 0	
Response	
Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	No
Document Name	
Comment	
NRG likes the approach of protecting communication links because you can identify the data, but at what point does the data transfer ownership from the responsible entity to the RC or BA (therefore, NRG also recommends that the SDT also definine the data to be protected). From that standpoint, additional requirement protections to be added into CIP-005 are recommended (by NRG) to protect the confidentiality and integrity of the data. NRG recommends working on a multiple approach to address the directive. The primary solution could address the protection of the communication link. As an alternative method, NRG recommends that the drafting team consider other methods that are not link level controls. Additionally, NRG asks that the drafting team provide clarity on the difference between “communication links” and “communication networks”.	
Likes 0	
Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8 - WECC	
Answer	No
Document Name	
Comment	
As written, it is unclear what constitutes a “communication link”, especially if that link is provided by a 3rd party. The standard should address the protection of the data.	
Likes 0	
Dislikes 0	
Response	
Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF	
Answer	No
Document Name	

Comment
The NSRF recommends focusing on the boundaries or interface points, not the links between control centers.

Likes 0	
Dislikes 0	

Response

Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	

Comment
SRP does not agree with the SDT's approach to focus the draft language on the protection of communication links. The focus of the draft language should be on both the communication links and the sensitive BES data, as required by FERC Order No. 822. The reliability of the communication links and integrity of sensitive BES data are critical to the reliability of the BES. SRP proposes merging the language that focuses on protection of communication with the language in the "Draft Guidance" section pertaining to the data-centric approach.

Likes 0	
Dislikes 0	

Response

Kelly Silver - Con Ed - Consolidated Edison Co. of New York - 1,3,5,6, Group Name Con Edison	
Answer	No
Document Name	

Comment
1. Recommend that the SDT focus on protecting the data for reliability and availability. 2. We recommend that this Standard not prescribe the method for protecting the data but the objective of reliability and availability as the focus. Alternative approaches of application security or communication security controls should be allowed and clearly addressed in the Requirements. The proposed procedures in Draft Language 1.1 and 1.2 would not be required.

3. FERC Order 822 section 58 clarifies this scope as inter-Control Center and intra-Control Center communications. The guidance seems to extend the scope beyond this

4. Recommend reviewing NIST Special Publication 800-47 which is titled Security Guideline for Interconnecting Information Technology Systems with a focus toward reliability and availability

5. The Standard should be an outcome-based Standard.

Likes 0	
Dislikes 0	

Response

Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body

Answer	No
Document Name	

Comment

Supporting APPA comments

Likes 0	
Dislikes 0	

Response

Andrew Gallo - Austin Energy - 1,3,4,5,6

Answer	No
Document Name	

Comment

This requirement should be drafted to allow Responsible Entities to implement an approach which fits the needs of its processes and infrastructure; allowing for either data and/or communication link protection.

Likes 0	
Dislikes 0	

Response

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	No
Document Name	
Comment	
TVA notes that within a cloud-based communications network such as the Internet, an MPLS network, a meshed network, or other non-point-to-point type of communications topology, it would be difficult to quantify a “link” as a physical or logical construct, as the “link” may be constructed of a virtual circuitry that traverses any number of underlying physical components. The language should be revised to focus on protecting information instead of antiquated notions of physical communication components associated with “links.” TVA is also concerned that the proposed language is vague enough to encompass transport links carrying an e-mail sent between two Control Centers, as no qualifications are provided regarding timeliness of the information. Should Internet based transport relay the e-mail, the registered entity would be obligated to protect, end-to-end, the Internet “data-links” connecting the two Control Centers. TVA suggests focusing on the “sensitive bulk electric system data” moving between Control Centers and not underlying communications infrastructure.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE	
Answer	Yes
Document Name	
Comment	
We support a path forward of focusing on protection of communication links with language to limit the scope of data to be protected with that data that does not have a shelf life or is considered perishable.	
Likes 0	
Dislikes 0	
Response	
Brandon Cain - Southern Company - Southern Company Services, Inc. - NA - Not Applicable - SERC	
Answer	Yes
Document Name	

Comment
Yes, Southern Company supports the SDTs approach focused on protection of communication links between Control Centers. Additionally, Southern requests the SDT to consider the providing clarifying language that ensures the proper scoping of this Standard to be “communications between Control Centers” and exclude their associated data centers. The definition of Control Center could inadvertently require additional protections be afforded to communications between an entity’s Control Centers and it’s own data centers, and that does not appear to be the intent stated in the FERC Order.

Likes 0	
Dislikes 0	

Response

Chris Scanlon - Exelon - 1,3,5,6	
Answer	Yes
Document Name	

Comment
See attachment Q1

Likes 0	
Dislikes 0	

Response

Mark Riley - Associated Electric Cooperative, Inc. - 1,3,5,6	
Answer	Yes
Document Name	

Comment
AECI agrees with the SDT's approach that the focus should be on the communication links rather than the sensitive BES data itself.

Likes 0	
Dislikes 0	

Response

Deborah VanDeventer - Edison International - Southern California Edison Company - 1,3,5,6 - WECC

Answer	Yes
Document Name	
Comment	
It is likely that the same types of logical controls would be utilized to protect either. It would be best to further the already established concept of protecting communication networks/links and explain how that, in turn, protects the data.	
Likes 0	
Dislikes 0	
Response	
Sheranee Nedd - Public Service Enterprise Group - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	
We agree with the approach to focus the draft language on the protection of the communication links. If the SDT decides to focus on the sensitive BES data, then a definition for “sensitive BES data” would need to be developed. The applicable requirements in IRO-10-2 and TOP-003-3 do not adequately address this.	
Likes 3	PSEG - Public Service Electric and Gas Co., 1, Smith Joseph; PSEG - PSEG Fossil LLC, 5, Kucey Tim; PSEG - Public Service Electric and Gas Co., 3, Mueller Jeffrey
Dislikes 0	
Response	
Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance	
Answer	Yes
Document Name	
Comment	
Perhaps the language should be edited in a manner that will allow entities to protect links and/or the sensitive BES data itself, allowing entities flexability in achieving the security objective.	
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 agrees with the approach that the focus of the protection should be on the communication links rather than the sensitive BES data itself.	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
CenterPoint Energy agrees that the focus should be on the protection of the communication link used to transport sensitive BES data and not the sensitive BES data itself. This aligns with the language in the FERC order “to require responsible entities to implement controls to protect, at a minimum, all communication links and sensitive bulk electric system data communicated between all bulk electric system Control Centers.”(FERC Order 822, P.41)	
Likes 0	
Dislikes 0	
Response	
Gerry Adamski - Essential Power, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lauren Price - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1,3,5,6	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Preston Walker - PJM Interconnection, L.L.C. - 2 - SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion	
Answer	
Document Name	
Comment	

1) Recommend that the SDT focus on protecting the data for reliability and availability

2) We recommend that this Standard not prescribe the method for protecting the data but the objective of reliability and availability as the focus. Alternative approaches of application security or communication security controls should be allowed and clearly addressed in the Requirements. The proposed procedures in Draft Language 1.1 and 1.2 would not be required.

3) FERC Order 822 section 58 clarifies this scope as inter-Control Center and intra-Control Center communications. The guidance seems to extend the scope beyond this

4) Recommend reviewing NIST Special Publication 800-47 which is titled Security Guideline for Interconnecting Information Technology Systems with a focus toward reliability and availability

5) The Standard should be an outcome based Standard. We like the option to protect either the data or the links. We would like to see these options clearly defined within the requirements and not just in the guidance. The Standard should be an outcome based Standard. FERC Order 822 section 58 clarifies this scope as inter-Control Center and intra-Control Center communications. The guidance seems to extend the scope beyond this by including references to DP's and listing Data links without reference to Control Centers.	
Likes 0	
Dislikes 0	
Response	

7. Do you agree with the security objective of the draft language? If not, please propose alternative language.

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority

Answer	No
Document Name	

Comment

It is the Entity's responsibility to protect its information systems, regardless of the origin of information that is fed info an information system. Specifically, the draft Guidance language directs REs to establish controls for data links between DPs and TOPs. In such a scenario, the DP may not be subject to any regulatory controls and the TOP has no mechanism to enforce what a DP is doing with their end of a communications link. Accordingly, the TOP is powerless to enforce end-to-end data link protections required by the draft language.

In the event that an RE has the ability to control data-link security end-to-end with other entities, such a protection still provides no inherent cyber security benefit for the information carried over the data link; the information itself may contain a malicious payload carried over an otherwise trusted data-link.

It is incumbent upon REs to configure information systems under their control to ensure that information provided to information systems is safe, trustworthy, and appropriately vetted; and potential for adverse impact of incomplete, untrustworthy, or malicious data has been appropriately mitigated. For example, on a Microsoft Windows server, the RE may install security patches that were downloaded from the public Internet. Such information is potentially adversely impactful to a BES Cyber System. However, the entity takes appropriate action to ensure the security patches are genuine. Even though communications links utilized for the vast majority of the transport are untrustworthy, appropriate application layer controls are leveraged to ensure the trustworthiness of the communications payload.

Likes 0	
Dislikes 0	

Response

Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body

Answer	No
Document Name	

Comment

Supporting APPA comments

Likes 0	
Dislikes 0	

Response

Preston Walker - PJM Interconnection, L.L.C. - 2 - SERC,RF	
Answer	No
Document Name	
Comment	
PJM proposes that the objective should focus on protecting the communication networks. Proposed language: “The Responsible Entity shall implement one or more documented plan(s) to protect data being transferred across communication networks between Control Centers, both inter-entity and intra-entity that include each of the applicable parts below:” The “Purpose” should include the security objective (confidentiality and integrity of data required for reliable operation of the BES).	
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	
Duke Energy does not disagree with the security objective to protect confidentiality and integrity of data required for reliable operation of the BES. We do not agree that the current draft language is measurable, and thus would make it difficult to audit. Moreoever, the draft language does not appear to fit the mold of other standards which are performance based. Also, more descriptive language needs to be placed in the requirement. Currently, as written, an entity would need to refer to the Guidelines and Technical Basis section to determine what was necessary to comply.	
Likes 0	
Dislikes 0	
Response	
Kelly Silver - Con Ed - Consolidated Edison Co. of New York - 1,3,5,6, Group Name Con Edison	
Answer	No
Document Name	
Comment	

We suggest "reliability and availability" replace "confidentiality and integrity" because EMS/SCADA systems are built on "reliability and availability." There should be flexibility when it comes to enforcing encryption and specifying methods and end points.

Likes 0	
Dislikes 0	

Response

Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8 - WECC

Answer	No
Document Name	

Comment

The security objective should be to protect the data.

Likes 0	
Dislikes 0	

Response

Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF

Answer	No
Document Name	

Comment

The security objective is not clearly stated. We recommend the drafting team put more emphasis or focus on the integrity of the data instead the confidentially. Additionally, we recommend a definition of data to be protected such as: Data if rendered unavailable, degraded, or misused within 15 minutes would adversely impact the Real-Time operation of the Bulk Electric System. Does this mean that everytime you do a database change, that change control per the CIP standards must be utilized? (for example, if the database is degraded, it may have a 15 minute impact).

Likes 0	
Dislikes 0	

Response

Jason Snodgrass - Georgia Transmission Corporation - 1

Answer	No
Document Name	
Comment	
Propose deleting reference of confidentiality in the standard and focus on integrity because adding confidentiality expands the scope of the FERC Directive.	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	No
Document Name	
Comment	
We suggest “reliability and availability” replace “confidentiality and integrity” because EMS/SCADA systems are built on “reliability and availability”.	
Likes 1	Illinois Municipal Electric Agency, 4, Thomas Bob
Dislikes 0	
Response	
Guy Andrews - Georgia System Operations Corporation - 3,4	
Answer	No
Document Name	
Comment	
Propose deleting reference of confidentiality in the standard and focus on integrity because adding confidentiality expands the scope of the FERC Directive.	
Likes 0	
Dislikes 0	
Response	

Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC	
Answer	No
Document Name	
Comment	
The commission is asking to implement controls to protect, at a minimum, the communication links and the data being communicated. The concepts introduced by the SDT (Confidentiality, Integrity, availability), are valid, but are not directly required by the commission. Also, the current CIPs do not mention those concepts. Either the requirements of the commission are updated or the SDT should fallback to the commission language.	
Likes 0	
Dislikes 0	
Response	
Deborah VanDeventer - Edison International - Southern California Edison Company - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
In regards to the objectives, confidentiality and integrity have not been stated as explicit objectives in the current Standards, although they are obviously implied. The security objective should align with the current standards – “to protect against compromise that could lead to misoperation or instability in the BES.”	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE	
Answer	No
Document Name	
Comment	
The language regarding physical security in the guidance section is concerning to Xcel Energy as physical security is not specifically referenced in the Standard or Requirement language. Cabling within an ESP spanning multiple PSPs is already required to be physically secured (or deploy alternative	

measures such as encryption) under CIP-006-6 R1.10, so requiring this on all wiring would greatly increase the scope of cabling beyond what is needed under CIP v6. If the SDT/FERC believes that all cabling in Control Centers need to be physically protected, then Xcel Energy would suggest the SDT update the existing language in CIP-006-6 R1.10 instead of through a new, separate, standard which raises the concern of double jeopardy and adds a new "spaghetti" requirement previously done away with by v5/v6. Xcel Energy suggests that the word 'confidentiality' be removed from draft language "*The Responsible Entity shall implement one or more documented plan(s) that achieve the security objective to protect* ***confidentiality*** *and integrity of data required for reliable operation of the BES"* to ensure consistency throughout the other CIP standards.	
Likes 0	
Dislikes 0	
Response	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	No
Document Name	
Comment	
MMWEC supports comments submitted by APPA.	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	No
Document Name	
Comment	

The security objective is not clearly stated. We recommend the drafting team put more emphasis or focus on the integrity of the data instead of the confidentially. Additionally, we recommend a definition of the data to be protected such as: Data if rendered unavailable, degraded, or misused within 15 minutes would adversely impact the Real-time operation of the Bulk Electric.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion	
Answer	No
Document Name	
Comment	
We suggest “reliability and availability” replace “confidentiality and integrity” because EMS/SCADA systems are built on “reliability and availability”.	
Likes 0	
Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	No
Document Name	
Comment	
AZPS does not agree with the security objective of the draft language as it is overly broad and extends beyond the scope of the directive set forth in Order 822 at Paragraph 53, which specifically targets data in transit between Control Centers. To the extent that this language is retained, AZPS recommends that the security objective be revised to state: “…achieve the security objective to protect confidentiality and integrity of data communicated between bulk electric system Control Centers and the associated communication links…”	
Likes 0	
Dislikes 0	

Response	
Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6	
Answer	No
Document Name	
Comment	
Tacoma supports the comments of Utility Services, Inc	
Likes 0	
Dislikes 0	
Response	
Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
SRP agrees with the security objective of protecting the confidentiality and integrity of data that is required for reliable operation and is transmitted between Control Centers.	
Likes 0	
Dislikes 0	
Response	
Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
If the security objective is to protect the confidentiality and integrity of operational reliability data transmitted between control centers, the NSRF agrees	
Likes 0	

Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
As it is understood, the objective is to ensure that data transmitted is received in a way that the recipient can be confident the data is complete and accurate.	
Likes 0	
Dislikes 0	
Response	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
In meeting the security triad of confidentiality, integrity, and availability, the security objective for availability is already addressed and monitored as noted under question 4. This requirement should be limited to the remaining two objectives of integrity and confidentiality.	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	

BPA agrees with the security objective but suggests that the supporting language needs to be modified to support the objective of protecting data rather than emphasizing protection of communication links. As discussed above, BPA also encourages the SDT to incorporate the requirements into existing CIP standards rather than creating a new standard. Wherever the requirements reside, BPA proposes the following edits to the draft SDT language:

The Responsible Entity shall implement one or more documented plan(s) that achieve the security objective to protect availability, confidentiality and integrity of data required for reliable operation of the BES. The plan applies to data being transferred across communication networks between Control Centers, both inter-entity and intra-entity and shall include each of the applicable parts below:

1.

i. *Identification of the data required for reliable operation of the BES (if not already identified under IRO-010-2 and TOP-003-3);*

ii. *Method(s) for protecting applicable data between Control Centers identified in 1.1, where technically feasible.*

iii. *Loss of protection of data should be alarmed to a central location with a method of timely response.*

Likes 0	
Dislikes 0	

Response

Candace Morakinyo - WEC Energy Group, Inc. - 3,4,5 - MRO,RF

Answer	Yes
Document Name	

Comment

Yes, the primary objective should be on protecting the data.

Likes 0	
Dislikes 0	

Response

Wendy Center - U.S. Bureau of Reclamation - 1,5

Answer	Yes
Document Name	

Comment	
Reclamation recommends adding the draft language to CIP-003-7i for low impact BES Cyber Systems, to CIP-005-5 for high and medium BES Cyber Systems, and to CIP-006-6 Requirement R1 Part 1.10 for physical security.	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
See attachment Q1	
Likes 0	
Dislikes 0	
Response	
Brandon Cain - Southern Company - Southern Company Services, Inc. - NA - Not Applicable - SERC	
Answer	Yes
Document Name	
Comment	
Southern Company agrees with the security objective of the draft language, but as previously stated, believes the language including the requirement to demonstrate confidentiality be removed. Although confidentiality is part of the foundational CIA security triad, in most instances confidentiality does not have a real-time (<15 minute) impact to the reliability of the BES.	
Likes 0	
Dislikes 0	
Response	
Charles Yeung - Southwest Power Pool, Inc. (RTO) - 2	

Answer	Yes
Document Name	
Comment	
If the security objective is to protect the confidentiality and integrity of operational reliability data transmitted between control centers, we agree.	
Likes 0	
Dislikes 0	
Response	
Andrew Gallo - Austin Energy - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1,3,5,6	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lauren Price - American Transmission Company, LLC - 1	
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	
Aaron Austin - AEP - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sheranee Nedd - Public Service Enterprise Group - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	
Likes 3	PSEG - Public Service Electric and Gas Co., 1, Smith Joseph; PSEG - PSEG Fossil LLC, 5, Kucey Tim; PSEG - Public Service Electric and Gas Co., 3, Mueller Jeffrey
Dislikes 0	
Response	

Anton Vu - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gerry Adamski - Essential Power, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Riley - Associated Electric Cooperative, Inc. - 1,3,5,6	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Kraft - Basin Electric Power Cooperative - 1,3,5,6	
Answer	Yes
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	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	

8. Is it clear what types of plans, procedures, and methods are needed to meet the draft language? If not, please propose alternative language.

sean erickson - Western Area Power Administration - 1,6

Answer	No
Document Name	

Comment

Referring to the protection of communication links, does this mean select individual links or does it really mean an entire network?

per the NSRF:The question assumes the development of a new standard. The NSRF believes the objectives can be met through simple clarifying language in CIP-002 and CIP-006. We believe the intent of the Order is met though other changes that have occurred in the standards over time. Confidentiality is appropriately addressed through the NERC ORD Confidentiality Agreement. The integrity of data is also addressed in multiple standards dealing with managing the quality of data used by operators (there are 136 references to data quality in the current set of standards).

Likes 0	
Dislikes 0	

Response

Charles Yeung - Southwest Power Pool, Inc. (RTO) - 2

Answer	No
Document Name	

Comment

The question assumes the development of a new standard. We believe the objectives can be met through simple clarifying language in CIP-002 and CIP-006. We believe the intent of the Order is met though other changes that have occurred in the standards over time. Confidentiality is appropriately addressed through the NERC ORD Confidentiality Agreement. The integrity of data is also addressed in multiple standards dealing with managing the quality of data used by operators (there are 136 references to data quality in the current set of standards).

Likes 0	
Dislikes 0	

Response

Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6

Answer	No

Document Name	
Comment	
Tacoma supports the comments of Utility Services, Inc	
Likes 0	
Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	No
Document Name	Project 2016-02 Communication Networks - Comment for Question 8.docx
Comment	
Please see the attached document for AZPS' comments regarding Question 8.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion	
Answer	No
Document Name	
Comment	
We do not agree with the draft language which focuses on networks. This language should focus on data. We like the option to protect either the data or the links. We would like to see these options clearly defined within the requirements and not just in the guidance. Replace “communication networks” with “communication networks or BES reliability data”. Include in 1.1 that this is for networks or data between Control Centers.	
Likes 0	
Dislikes 0	
Response	

David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	No
Document Name	
Comment	
MMWEC supports comments submitted by APPA.	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE	
Answer	No
Document Name	
Comment	
This question can only be answered once a determination has been made as to whether a new standard is going to be created or updates are made to existing standards.	
Likes 0	
Dislikes 0	
Response	
Candace Morakinyo - WEC Energy Group, Inc. - 3,4,5 - MRO,RF	
Answer	No
Document Name	
Comment	
A CIP-005 requirement for physical protection or encryption of data flowing between ESPs associated with High and/or Medium Impact BES Cyber Systems should be sufficient to address this need.	
Likes 0	

Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	
The openness left to entities allows flexible solutions that would be more appropriate than prescriptive requirements would allow. This flexibility leaves concerns to what degree it would be audited to, this is similar to the Low Impact requirements.	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	No
Document Name	
Comment	
We like the option to protect either the data or the links. We would like to see these options clearly defined within the requirements and not just in the guidance. Replace “communication networks” with “communication networks or BES reliability data”. Include in 1.1 that this is for networks or data between Control Centers.	
Likes 1	Illinois Municipal Electric Agency, 4, Thomas Bob
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	No
Document Name	

Comment
Please see Texas RE's comment in response to Question 6.

Likes 0	
Dislikes 0	

Response

Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8 - WECC

Answer	No
Document Name	

Comment
Delete 1.1 1- Define the boundaries of communication networks transmitting data required for reliable operations. 2- Method(s) for protecting the in scope data between Control Centers where technically feasible.

Likes 0	
Dislikes 0	

Response

Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF

Answer	No
Document Name	

Comment
The question assumes the development of a new standard. The NSRF believes the objectives can be met through simple clarifying language in CIP-002 and CIP-006. We believe the intent of the Order is met though other changes that have occurred in the standards over time. Confidentiality is appropriately addressed through the NERC ORD Confidentiality Agreement. The integrity of data is also addressed in multiple standards dealing with managing the quality of data used by operators (there are 136 references to data quality in the current set of standards).

Likes 0	
Dislikes 0	

Response

Kelly Silver - Con Ed - Consolidated Edison Co. of New York - 1,3,5,6, Group Name Con Edison	
Answer	No
Document Name	
Comment	
Language should focus on data, not networks. There should be flexibility when it comes to enforcing encryption and specifying methods and end points.	
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	
Duke Energy suggests the drafting team consider the balance between existing CIP requirements, and the proposed requirement to protect and encrypt communication paths. There are existing CIP requirements in CIP-005-5 that certain communications links be inspected for malicious code for inbound and outbound communications. If a communication link is now expected to be encrypted, the ability to inspect the traffic for malicious code will not be feasible. If an entity determines that encryption is therefore not a possible option to be able to maintain compliance with existing requirements, the only suggested protection mechanism left would be physical and is not feasible in most situations.	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	
CenterPoint Energy has concerns with implementing methods for protecting communication links between Control Centers (R1.3) in situations where the end point is not owned by the entity. What would be the compliance implications if the owner of the end point is not willing to implement	

protections? CenterPoint Energy recommends that the drafting team provide guidance around ownership of communication links and how to comply with the requirement in these situations.	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	No
Document Name	
Comment	
Supporting APPA comments	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	No
Document Name	
Comment	
The responsibilities assigned to REs potentially cover information systems for which the RE has no control, creating compliance obligation that would be impossible to satisfy.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE	
Answer	Yes
Document Name	

Comment
We also believe sub Requirements 1.1 and 1.2 look as if they can be consolidated. Proposed language follows at the end of this response. Possible Alternative Language: **R1.** The Responsible Entity shall implement one or more documented plan(s) that achieve the security objective to protect confidentiality and integrity[1] of data required for reliable operation of the BES. The plan applies to data being transferred across communication networks between Control Centers, both inter-entity and intra-entity and shall include each of the applicable parts below: **R1.1** Procedure(s) to identify networks requiring protections, and their associated boundaries. **R1.2** Procedure(s) to associate the categorization completed under CIP-002-5.1a with the identified networks in R1.1. **R1.3** Procedure(s) to design, construct, and implement protections for the networks identified in R1.1. The procedure shall be tailored to address the high, medium, and low impact risks associated with the networks in R1.2. **R1.4** Procedure(s) to address protections for networks identified in R1.1 where technically feasible. [1] NIST Special Publication 800-53A : Revision 4, Appendix B (Glossary) **[NIST incorporates by reference the definition found in U.S. Code, Coordination of Federal Information Policy, Information Security (44 U.S.C. §3542), defining "integrity" as "Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity."**]

Likes 0	
Dislikes 0	

Response

Mike Kraft - Basin Electric Power Cooperative - 1,3,5,6	
Answer	Yes
Document Name	

Comment
Basin Electric would prefer the plans, procedures and methods be included in CIP-003 and CIP-005 as appropriate vs. in the new proposed standard CIP-012.

Likes 0	
Dislikes 0	

Response

Chris Scanlon - Exelon - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
See attachment Q1	
Likes 0	
Dislikes 0	
Response	
Sheranee Nedd - Public Service Enterprise Group - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	
For requirement 1.3, we recommend adding the bulleted list from the Draft Guidance Section (similar to CIP-006-6 R1.10) into the requirement language. The requirement would be written as follows: **1.3** Method(s) for protecting communication networks between Control Centers identified in 1.1, where technically feasible. The Responsible Entity shall document and implement one or more of the following: • Site to site encryption; or • Application layer encryption; or • Physical protections.	
Likes 3	PSEG - Public Service Electric and Gas Co., 1, Smith Joseph; PSEG - PSEG Fossil LLC, 5, Kucey Tim; PSEG - Public Service Electric and Gas Co., 3, Mueller Jeffrey
Dislikes 0	
Response	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	

Comment	
ERCOT requests that the SDT also consider guidance on where parties at either end of a communication link are not in agreement.	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
It is important to maintain flexibility for Responsilbe Entities to develop controls that work best within their environment and for their situation. The less prescriptive the requirements, the more flexible and agile the Responsible Entity can be to work within the skills sets of their personnel and respond to the changing security and technology landscapes. IPC suggests that the requirements state objectives and requirements to document positions and controls and be less prescriptive than the CIP standards are in their current state.	
Likes 0	
Dislikes 0	
Response	
Brandon Cain - Southern Company - Southern Company Services, Inc. - NA - Not Applicable - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 1,5	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Riley - Associated Electric Cooperative, Inc. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gerry Adamski - Essential Power, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Guy Andrews - Georgia System Operations Corporation - 3,4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Austin - AEP - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jason Snodgrass - Georgia Transmission Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lauren Price - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 1,3,5	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Preston Walker - PJM Interconnection, L.L.C. - 2 - SERC,RF	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Andrew Gallo - Austin Energy - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

9. The SDT uses the term “communication networks” throughout the draft language including an obligation to define the boundaries of such communication networks. Does the SDT need to define the term for inclusion in the NERC Glossary of Terms? If so, please propose a definition of “communication networks.”

Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body

Answer	No
Document Name	

Comment

Supporting APPA comments

Likes 0	
Dislikes 0	

Response

Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	No
Document Name	

Comment

CenterPoint Energy recommends using the term “communication link(s)” instead of “communication networks” in the requirement language to align with the FERC directive. The term “communication networks” can encompass many types of networks, some of which are currently out of scope for the CIP Standards. CenterPoint Energy believes the focus should be on the protections around the communication links used to transmit sensitive bulk electric system data between Control Centers. CenterPoint Energy recommends the following changes:

*“The Responsible Entity shall implement one or more documented plan(s) that achieve the security objective to protect confidentiality and integrity of data required for reliable operation of the BES. The plan applies to data being transferred across communication **links** between Control Centers, both inter-entity and intra-entity and shall include each of the applicable parts below:*

*1.1 Procedure(s) to identify the communication **links** requiring protections;*

*1.2 Procedure(s) for defining the boundaries of communication **links** transmitting data required for reliable operation identified in 1.1, if applicable;*

*1.3 Method(s) for protecting communication **links** between Control Centers identified in 1.1, where technically feasible.”*

Likes 0	
Dislikes 0	

Response

Preston Walker - PJM Interconnection, L.L.C. - 2 - SERC,RF	
Answer	No
Document Name	
Comment	
PJM asserts that “between Control Centers” already clarifies the scope.	
Likes 0	
Dislikes 0	
Response	
Kelly Silver - Con Ed - Consolidated Edison Co. of New York - 1,3,5,6, Group Name Con Edison	
Answer	No
Document Name	
Comment	
CIP-002 Exemptions already utilize the "communications networks" term. However, consider that the FERC Order Section 58 clarifies the focus and the scope on inter-Control Center and intra-Control Center communications	
Likes 0	
Dislikes 0	
Response	
Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
Draft language, applicable part 1.1 call for procedure(s) to identify the communications network requiring protections. A defined term for communication network may restrict an entity’s flexibility in determining how to implement the draft language.	
Likes 0	

Dislikes 0	
Response	
Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF	
Answer	No
Document Name	
Comment	
The term "communication networks" is used elsewhere in the standards. The NSRF believes that defining the term for one standard would have unintended impacts on other standards.	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4	
Answer	No
Document Name	
Comment	
Does not need to be defined, because from a simple view it includes everything outside the CIP ESP.	
Likes 0	
Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8 - WECC	
Answer	No
Document Name	
Comment	

The standard uses two terms; "communication networks" and "communication links". Use one term, not two. We believe the standard should address securing the data, not the "networks" or "links".	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	No
Document Name	
Comment	
Recommend a NO vote on defining “communication network” But consider that the FERC Order Section 58 clarifies the focus and the scope on inter-Control Center and intra-Control Center communications	
Likes 1	Illinois Municipal Electric Agency, 4, Thomas Bob
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	
The term “communication networks” is used elsewhere in the standards. The NSRF believes that defining the term for one standard would have unintended impacts on other standards.	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE	

Answer	No
Document Name	
Comment	
The term communication Networks has many different applications and is too broad of a term to be used in in Standard Language without adding a defined term in the NERC Glossary. The FERC directive only references “Links.” Xcel Energy would suggest formal definitions be drawn up for both Communication Networks and Links.	
Likes 0	
Dislikes 0	
Response	
Mark Riley - Associated Electric Cooperative, Inc. - 1,3,5,6	
Answer	No
Document Name	
Comment	
The term "communication networks" is already used in the applicability section of the CIP standards. Defining this term could have unintended consequences.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion	
Answer	No
Document Name	
Comment	
Recommend a NO vote on defining “communication network”. But consider that the FERC Order Section 58 clarifies the focus and the scope on inter-Control Center and intra-Control Center communications.	
Likes 0	
Dislikes 0	

Response	
Brandon Cain - Southern Company - Southern Company Services, Inc. - NA - Not Applicable - SERC	
Answer	No
Document Name	
Comment	
Southern Company respectfully requests that the SDT refrain from attempting to define “communications networks” as an attempt could be defined so broadly to open the door to varying degrees of interpretation, or alternatively a restrictive definition could place limitations on a Responsible Entity’s implementation. The language, as specified in R1.2, places the responsibility on the Entity to define “the boundaries of *communication networks transmitting data* required for reliable operation” and should be determined by the Entity without the need for another defined term.	
Likes 0	
Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	No
Document Name	
Comment	
AZPS recommended in its response to Question 8 that the term “communication networks” be replaced with the term “communication links.” AZPS recommends that the term “communication links” be defined as: The logical communication path that uses a routable protocol to connect BES Control Centers and over which Sensitive BES Data is transmitted. If the term “communication network” is retained, AZPS recommends the same definition: The logical communication path that uses a routable protocol to connect BES Control Centers and over which Sensitive BES Data is transmitted.	
Likes 0	
Dislikes 0	
Response	
Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6	
Answer	No

Document Name	
Comment	
Tacoma supports the comments of Utility Services, Inc	
Likes 0	
Dislikes 0	
Response	
Charles Yeung - Southwest Power Pool, Inc. (RTO) - 2	
Answer	No
Document Name	
Comment	
The phrase “communication networks” is used elsewhere in the standards. To define the term for one standard would have unintended impacts on other standards.	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1,3,5,6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lauren Price - American Transmission Company, LLC - 1	
Answer	No

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gerry Adamski - Essential Power, LLC - 5	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Kraft - Basin Electric Power Cooperative - 1,3,5,6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
TVA suggests focusing on the “sensitive bulk electric system data” moving between Control Centers and not underlying communications infrastructure.	

Likes 0	
Dislikes 0	
Response	
Andrew Gallo - Austin Energy - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	
“A collection of interconnected components utilized for transmitting and/or receiving data.”	
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 supports a definition of “communication networks”. Use of the term “communication” creates some ambiguity, particularly what types of communication this applies. It is not known if all forms of communication fall under this purview, specifically verbal communication avenues.	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	

The collection of networked communication devices that provide routable transmission of data.	
Likes 0	
Dislikes 0	
Response	
Richard Kinas - Orlando Utilities Commission - 3,5	
Answer	Yes
Document Name	
Comment	
Communication networks - Any technology that allows the transfer of information and data, including voice, between two endpoints.	
Likes 0	
Dislikes 0	
Response	
Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
NRG recommends that the SDT provide a defined term for “Communication Networks” into the the NERC GOT.	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	

Comment
Texas RE would support the SDT in defining the term “communication networks”. In addition, Texas RE recommends adding the following to the list of examples of communication links: Data link(s) between a Generator Operators.

Likes 0	
Dislikes 0	

Response

Jason Snodgrass - Georgia Transmission Corporation - 1	
Answer	Yes
Document Name	

Comment
Proposed definition - Communication network is data link used to connect one location to another location for the purpose of transmitting and receiving digital data used in intra-Control Center communications for reliability operations of the BES.

Likes 0	
Dislikes 0	

Response

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

Comment
IPC suggests communication networks be defined as, "Those networks used to logically and physically transport a communications link."

Likes 0	
Dislikes 0	

Response	
Aaron Austin - AEP - 3,5	
Answer	Yes
Document Name	
Comment	
AEP believes this will help define the extent of the requirements.	
Likes 0	
Dislikes 0	
Response	
Guy Andrews - Georgia System Operations Corporation - 3,4	
Answer	Yes
Document Name	
Comment	
Proposed definition - Communication network is data link used to connect one location to another location for the purpose of transmitting and receiving digital data used in intra-Control Center communications for reliability operations of the BES.	
Likes 0	
Dislikes 0	
Response	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
ERCOT asserts that “networks” may be too broad and implicate unintended equipment based on a common understanding of the term. Consider the use of “Communication Link” instead. Proposed definition: communications infrastructure between two or more locations for the purpose of transmitting and receiving data.	

Likes 0	
Dislikes 0	
Response	
Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC	
Answer	Yes
Document Name	
Comment	
A definition of “communication networks” should be provided in the context of the CIP standard. This would minimize the risk of miss interpretation by the entities. In this case, we think that part of the definition should mention the logical network, not the physical network (not the equipment). So the definition could be logical network that is being used to transport data used by the BES	
Likes 0	
Dislikes 0	
Response	
Sheranee Nedd - Public Service Enterprise Group - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	
We recommend the following definition: Communication Network: a system of sending and receiving information, i.e. data, from point A to point B using a network of logical and physical devices. The term ‘communication network’ excludes equipment facilities used exclusively for Interpersonal Communication or Alternative Interpersonal Communication, as defined in the NERC Glossary of Terms.	
Likes 3	PSEG - Public Service Electric and Gas Co., 1, Smith Joseph; PSEG - PSEG Fossil LLC, 5, Kucey Tim; PSEG - Public Service Electric and Gas Co., 3, Mueller Jeffrey
Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	

Comment	
Yes – Clarity is always welcomed.	
Likes 0	
Dislikes 0	
Response	
Deborah VanDeventer - Edison International - Southern California Edison Company - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
If the term “communication networks” is not formally defined, industry interpretations will vary widely.	
Likes 0	
Dislikes 0	
Response	
Candace Morakinyo - WEC Energy Group, Inc. - 3,4,5 - MRO,RF	
Answer	Yes
Document Name	
Comment	
The SDT needs to make it clear whether there are deliniations / transitions between routable and other forms (serial, dial-up) forms of communication network. They should also make it clear what specific protections apply to those parts of the communication network over which a Registered Entity has direct control (up to and including the ESP) and those parts over which a Registered Entity may have little or no control (e.g. network communication links between ESPs).	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 1,5	

Answer	Yes
Document Name	
Comment	
To promote consistency as the standards change, Reclamation recommends NERC define “communication network” in the NERC Glossary of Terms. Reclamation recommends the following definition of Communication Network: “A system of communication connections consisting of (but not limited to) cables, fibers, microwave radio links, satellites, etc. used to connect computers or other terminals for the purpose of exchanging data required for the reliable operation of the BES.”	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
See attachment Q1	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE	
Answer	Yes
Document Name	
Comment	
We support a NERC Glossary Term for “Communication Network.” Suggested Definition	

Communication Network – Logical connections between two or more control centers which pass real time operational reliability data required for reliable operation of the Bulk Electric System. The connections may include, but are not limited to, physical equipment, through tunneling, or other virtual constructs. Potential GTB support: The Communication Network is a layer 3 (network layer) construct as established by the International Organization for Standardization (1989-11-15). "ISO/IEC 7498-4:1989 -- Information technology -- Open Systems Interconnection -- Basic Reference Model: Naming and	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	Yes
Document Name	
Comment	
The document continually uses the terms, “communication links”, “communication networks”, “data links”, “in-scope communication networks”, “in-scope communication links”, and in one case “communication networks/data links”, without clarifying the differences between any of the terms, or their intended use. This adds ambiguity to the document. Questions surface regarding the nature of a link being a single path, and do multiple links form a network? What is the difference between a communication link and a data link, does one carry voice traffic and the other does not? Do “in-scope” vs. “not in-scope” links or networks need to be identified separately? If the terms are being used interchangeably, then the correct term and its definition needs to be identified and used consistently.	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Additional comments received by Chris Scanlon of Exelon

Questions

1. The SDT asserts that the referenced data is already afforded protections at rest under existing CIP standards (CIP-003, 005, 007, etc.), perishable, and has a diminished need for protection over time. Do you agree with the SDT's assertion? If you agree, please supply a rationale to support the position.

☒ Yes
☐ No

Comments: Exelon agrees that the referenced data is already afforded protections at rest under the existing CIP Standards through physical and logical protections. The standards use a layered defense-in-depth approach based on the impact rating of the BES Cyber Systems. For example, for the BES Cyber Systems that communicate with a routable protocol using External Routable Connectivity, more granular security controls are applied to those BES Cyber Systems from CIP-005-5, CIP-006-6, CIP-007-6, and CIP-010-2. Whereas for those BES Cyber Systems that do not communicate externally, the CIP-006-6 standards affords specific physical security controls to "restrict physical access" along with the logical controls from CIP-007-6 and CIP-010-2 to support, malicious code prevention, security patch managements, configuration baselines, etc.

There is also a diminished need to protect real-time reliability operating data over time given that it is only used for real-time operation at a point-in-time. Once it is replaced by newer information, there is less of a need to protect the referenced data over time.

Additional thoughts & General Comments:

1) There is a disconnect between the requirement language and the Guidelines and Technical Basis (GT&B) section. The following examples identify specific instances where the GT&B and requirement language are inconsistent.

a. The draft requirement describes the applicable communication networks as those transmitting "data required for reliable operation of the BES" whereas the guidance refers to networks that transmit "operational reliability data between Control Centers." The former indicates a measure of Responsible Entity discretion in identifying the critical networks, whereas the latter would seem to capture any network transmitting operational reliability data, regardless of the effect of that data on reliable operation.

The guidance later refers to identifying "communication links that could adversely impact the reliable operation of the Control Center within 15 minutes." That seems to push for a measure of entity discretion in designing a process for identifying such networks and conflict with the identification of all networks that transmit "operational reliability data between Control Centers

b. The GT&B section uses wording such as "required" or "must" which is requirement language and not guidance. The GT&B is to explain the requirement language.

c. The GT&B states that "the Responsible Entity should ensure that the methods chosen include rationale supporting the identification of such communication networks" however the Requirement only states that there be "1.1 Procedure(s) to identify the communication networks requiring protections."

d. The GT&B suggests that a "Responsible Entity complement physical protections with logical protections to fully ensure that the integrity and confidentiality of data transmitted between Control Centers is protected." Are there cases where physical security would not be sufficient thereby making this a requirement to achieve the security objective.

e. The GT&B suggests that "the Responsible Entity must document and implement plans for the protection of the confidentiality and integrity of operational reliability data communicated between Control Centers." We are obligated to demonstrate that we have implemented the Plan(s), but this reads as if we have to have separate evidence that demonstrates the plans that were used to implement.

2) What does it mean for a communication network to be within an entity's "footprint"? Does that refer to networks within a retail distribution area? Does that refer to communication networks at an entity's facility? If it is associated with the" utility footprint", how does that concept apply to entities without a traditional utility "footprint" such as a GOP or RC?

3) The GT&B should specifically state that a Responsible Entity that lacks a Control Center is not subject to the Standard. For example, a GOP with only a control room for a single generating facility location would not have a "Control Center" and would not therefore be subject to the Standard. From a compliance perspective, it is helpful when the guidance says this explicitly.

4) By definition, only RCs, BAs, TOPs, and GOPs can have "Control Centers" yet the CIP Standards generally apply the DPs, TOs, GOs, and IAs as well. Are these latter entities exempt from the Standard?

5) The application of the Standard to protect communications networks should not inhibit an entity's ability to participate in programs (e.g. anti-terrorism, CRISP, etc.) where network connections to government or other entities are necessary to share information. The GT&B should provide guidance supporting that the protections of communications are not intended to inhibit these types of data monitoring activities or with the confidentiality and data integrity required by the Standard.

6) Addressing the need to clearly scope this Standard to ESP to ESP networks.

Below is discussion for allowing the Control Center to Control Center links assessed for this requirement in 1.1 to be able to be limited by a registered entity to Control Center ESP to Control Center ESP links (inter and intra). We would prefer to see the scope more defined within the Standard, but would at a minimum expect to see more clarity within the Guidance.

a. The guidance suggests the possibility of using NERC CIP-002 criteria to identify all inter-Control Center and intra-Control communication links. "As one possible solution, the Responsible Entity could apply CIP-002 criteria to identify all inter-Control Center and intra-Control

Center communication links that could adversely impact the reliable operation of the Control Center within 15 minutes." By application of the existing NERC CIP standards the CIP-002 criteria would identify communication links between ESPs (inter and intra Control Center).

There is an assumption statement that the SDT makes that is only true if the links are limited to ESP to ESP. "The SDT asserts that the referenced data is already afforded protections at rest under existing CIP standards (CIP-003, 005, 007, etc.), is perishable, and has a diminished need for protection over time. ". Non ESP devices holding operational data at rest may not be currently protected as part of NERC CIP standards as they are not in NERC CIP Scope. Example: PMU data transmitted between Control Centers but not having 15 minute impact.

b. Providing communications protections in this standard to non ESP to ESP links would mean that we are protecting networks under the rigor of this new NERC CIP standard without protecting the end devices (endpoints) under the NERC CIP requirements. By not using the same criteria there is risk to performers dealing with additional complexities of the NERC CIP standards and there is risk that auditors would initially interpret the end devices of these protected networks as being misclassified. The NERC CIP Standards determine the NERC CIP devices and the ESPs protecting those devices with a 15 minute impact criteria. The initial scope of the communications network requirements reasonably would be limited to links between those protected devices.

c. If planning and operational data without a 15 minute criterial is required to be in this standard then the standard needs more than network communications to ensure the standards cover that protection, it would require additional device protections.

d. With this allowed limitation of ESP to ESP links the issues related to a lack of clarity of "communication networks", "communication links", "sensitive bulk electric system data" are reduced as the scope of the protected networks is easily defined.

2. If you do not agree with the SDT's assertion in Question 1, please identify the type of data, the risk posed at rest, and supply the rationale to support the position.

   Comments:

   Not Applicable.

3. Future enforceable Reliability Standards IRO-010-2 and TOP-003-3 identify "data required for reliable operation." For example, Requirement R1 of IRO-010-2 states:

R1. The Reliability Coordinator shall maintain a documented specification for the data necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments. The data specification shall include but not be limited to:

1.1. A list of data and information needed by the Reliability Coordinator to support its Operational Planning Analyses, Real-time monitoring, and Realtime Assessments including non-BES data and external network data, as deemed necessary by the Reliability Coordinator.

TOP-003-3 Requirements R1 & R2 also have similar requirements for BAs and TOPs.

Do you agree that outlining this approach for identifying "data required for reliable operation" in the Guidelines and Technical Basis is sufficient; consequently, an additional definition of "sensitive BES data" or a requirement to identify "sensitive BES data" is not necessary? If not, please explain.

☐ Yes
☐ No

Comments: Exelon does not agree with placing the obligation for what data is to be considered should be placed into the GT&B. Exelon does support leveraging existing descriptions of data required for reliable operation as much as possible so that data classified is consistent across the Standards. For entities covered by IRO-010 and TOP-003, CIP-012 should include in the Requirement language which data is required for protection. Having different groups of reliability data for the same entities will make compliance efforts needlessly complex with no added benefit to reliable operation.

4. The SDT asserts that "availability" of inter-and intra-entity Control Center communication of data is being addressed in Project 2016-01 Modifications to TOP and IRO Standards, specifically Reliability Standards TOP-001-4 and IRO-002-5. The proposed standards require redundant and diversely routed data exchange capabilities at a Responsible Entity's primary Control Center. Do you agree that "availability" is adequately addressed by these standards? If not, please provide rationale to support your position.

☐ Yes
☐ No

Comments: Exelon agrees that the separate "Project 2016-01 Modifications to TOP and IRO Standards" covers the availability of the referenced data. In addition, covering the availability of data in this project goes beyond the scope of the Commission's directive, which is addressed only at protecting communication links and data for confidentiality and integrity.

5. The SDT is proposing to develop a new CIP standard because the directives of FERC Order 822 related to the protection of communication networks used to exchange sensitive BES data regardless of the entity's size or impact level. Do you agree with the drafting of a new CIP standard to address this issue? If you disagree and would prefer to include requirements in existing CIP Standards, such as CIP-003 and CIP-005, please provide rationale and propose requirement language.

☒ Yes
☐ No

Comments: Exelon agrees that the directive should be addressed through a new Standard, as proposed by the SDT. The other CIP Standards exempt "Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters." Revising those Standards to cover this new topic would require revisiting those exemptions in each Standard. It may be simpler to use an entirely specific Standard rather than re-opening the exemption for each existing CIP Standard.

6. The SDT evaluated multiple approaches to addressing the directive. The approach proposed in this informal posting focuses on the protection of communication links. An alternative approach could focus on the protection of the sensitive BES data itself. Do you agree with the SDT's approach to focus the draft language on the protection of communication links? If not, please provide rationale and propose alternative language.

☒ Yes
☐ No

Comments: Exelon supports responding to the directive by focusing on protecting the confidentiality and integrity of data sent over communication links; thereby applying protections to the data by addressing the communication links.

Exelon would prefer to change the "where technically feasible" language to "based on Cyber Asset capability." The version 5 set of Standards introduced the notion that there may be limitations to Cyber Assets and the SDT reduced the number of instances associated with Technical Feasibility Exceptions (TFE). For example, Requirement 1.3 could be rewritten to state: "Method(s) for protecting communication networks between Control Centers identified in 1.1, based on Cyber Asset **capability**." This would imply documenting the lack of capability but not require a TFE. Nearly any mitigating measures that would be required for a TFE could be considered protections that are documented to meet this requirement.

Exelon appreciates the SDT adding examples to the GT&B about approaches that can be implemented to meet the obligation of protecting communication networks. Exelon recommends that the SDT consider adding some text regarding the feasibility of these methods to the GT&B and whether the feasibility would ultimately affect whether the method would be viable:

- Site to site encryption – this is the most feasible approach at this time and focuses the protections on the end-points of the communications networks directly that make up the site-to-site encryption. Additionally, with this approach, there would not need to be an analysis of any of the intermediate communication networks or the transport layer communication networks since the site-to-site encryption protects the entire communication path.

- Application layer encryption – there are several barriers that would make this approach unlikely for mass use:
  - Lack of support – most vendors do not have these capabilities nor have them on their roadmaps
  - Lack of standards – if a vendor has application layer encryption it is most often proprietary
  - Lack of depth – some of the solutions that use SSL or TLS and all but TLS 1.2 have been deprecated.

  Once standards have been created for an interoperable application layer encryption protocol that also includes reliability and integrity features, then this would be the long range goal. This would provide the highest level of transport protections from device to device.
- Physical protections – depending on the size of the entity, deploying physical protections sufficient to protect the confidentiality and integrity of the referenced data, this may not be a feasible approach due to the cost of retrofitting and the limited protection it provides. It may be useful for short runs but as an overall approach may not possible.

7. Do you agree with the security objective of the draft language? If not, please propose alternative language.

   ☐ Yes
   ☐ No

   Comments: Exelon agrees with the security objective to protect communication networks between Control Centers. Exelon agrees with the security objective, however, requests the SDT add more clarity to the requirement language for what communication network end-points are actually expected to be protected and whether every intermediate communication network is required to be protected when implementations such as application-layer security or site-to-site virtual private networks are used.

8. Is it clear what types of plans, procedures, and methods are needed to meet the draft language? If not, please propose alternative language.

   ☐ Yes
   ☐ No

   Comments: The current draft language is reminiscent of V3 CIP-002 with entities determining their own risk based method without the guidance of a bright line. That did not work well to bring consistent implementation and left entities and regions unevenly protected. Defining the data to be protected as that which is transmitted between Control Center ESP to Control Center ESP (for High and Medium) does allow that bright line. If specific details related to the applicable protections are included in Guidance only, there will be

significant different interpretations. Exelon's preference would be to see more specificity within the Standard language itself. For entities without Electronic Security Perimeters, it is important to identify what end points need to be protected within the communication networks.

Implementation of Protections

1) Given proposed application to "inter-entity" communication networks, how will differences between entities be handled? For example:

a. If two entities take different approaches to encryption, how should that be resolved? Will there be dispute resolution of some kind?

b. What if one entity's approach is considerably more expensive and raises questions on prudency? How should that be resolved, particularly if utilities are in different states or have different rate structures that might not provide for the recovery of these costs?

c. If two entities have different opinions on whether their connecting communication network needs to be protected, whose view prevails?

i. Always the most conservative (protective) entity?

ii. Or is the Responsible Entity that identified the network as critical the only entity that needs to demonstrate compliance? If so, how can the other entity be required to undertake the costs necessary to assist the first entity in demonstrating compliance? (In other words, if I don't see a network as critical, why and how can I be required to spend money to assist you in implementing expensive encryption for purposes of your compliance?)

2) The guidance should expand on what is meant by "confidentiality" and "integrity" to ensure that auditors and Responsible Entities do not have different understandings of what the Standard is intended to accomplish.

- The reference to NIST Special Publication 800-53A is helpful, but it is not clear whether or not the Standard is specifically incorporating the definition of "integrity" contained in that publication. That publication also defines "confidentiality" but in a manner that includes personal data not relevant to NERC compliance.
- If the reference to NIST Special Publication 800-53A is intended to guide implication of the Standard in other ways, the guidance should explain how the NIST document is relevant. It appears to be focused on the assessment of confidentiality and integrity controls rather than the design of such controls.

3) The guidance states that physical conduit "can be used," but also suggests that conduit be supplemented by logical protections. Using conduit with additional logical controls might be a good security practice, but the Standard should specify that the use of physical conduit is sufficient to comply with the Standard. As written, it could be read that physical conduit, on its own, may not be sufficient for compliance.

4) Other than "site-to-site encryption" and "application layer encryption" are there other logical methods to protect data confidentiality and integrity that should be described in the program? The guidance does not limit Responsible Entities to those methods, but it can help from an audit perspective if the methods we use are described in the guidance.

9. The SDT uses the term "communication networks" throughout the draft language including an obligation to define the boundaries of such communication networks. Does the SDT need to define the term for inclusion in the NERC Glossary of Terms? If so, please propose a definition of "communication networks."

☐ Yes
☐ No

Comments: To ensure there is clear understanding of what communication networks are intended to be protected, the term "communication networks" should have a NERC defined definition. As written, the requirements and GT&B appear to commingle at what point of the "communication networks" are protections to be afforded. For example, the requirement "**1.1 Procedure(s) to identify the communication networks requiring protections**" obligation doesn't provide sufficient understanding of how to make that identification. Is the communication network that is local to the facility to be included, the communication network that is associated with the wide area network, or both. Moreover, requirement "**1.2 Procedure(s) for defining the boundaries of communication networks transmitting data required for reliable operation identified in 1.1, if applicable**" requires the entity to establish some boundary, but no clarity on how or what is an appropriate boundary. If an entity choses the boundary at the Electronic Security Perimeter to another Electronic Security Perimeter only, would that sufficiently addresses the security objective of the requirement?

The GT&B states that "The plan(s) should identify the applicable communication networks both within the entity's footprint, and any applicable networks between Responsible Entities." This statement adds additional ambiguity as to what points of the communication network are to be protected. If the Plan(s) are to take into account other networks "between Responsible Entities" does this also include the

telco provided networks? Depending on the solutions used, the intermediate communication networks are not a risk and are just the transport layer for the encrypted data packets.

Additional comments received from Vivian Vo of APS (Q8)

No, AZPS respectfully submits that the draft language is not clear relative to the types of plans, procedures, and methods that are needed for compliance therewith. In particular, AZPS has identified several revisions to the draft language that should be implemented to ensure clarity and consistency relative to the obligation being described:

- Evaluate and revise the introductory language to ensure that it is consistent with the content of the subparts;
- Replace the term "communication networks" with the term "communication links;" and
- Develop appropriate defined terms to ensure that the responsible entities have a clear and unambiguous scope and associated expectations and obligations (e.g., the term "communication networks" and the scope of data to which these requirements are applicable).

AZPS recommends these revisions as they will further ensure that the protections required by the FERC directive are clear and unambiguous and that protections are applied more uniformly across entities that communicate via the in-scope data links. Without such modifications, ambiguity coupled with the inherent complexity of the processes and data that are in-scope will create unnecessary risk and diminish the value and benefit of the protections implemented to the reliable operation of the BES.

AZPS recommends the following modifications to the draft language:

The Responsible Entity shall implement one or more documented plan(s) that ~~achieve the security objective to protect confidentiality and integrity of data required for reliable operation of the BES. The plan~~ applies to data being transferred across Communication ~~networks~~Links between Control Centers, both inter-entity and intra-entity, and that shall include each of the applicable parts below:

1.1 Procedure(s) to ~~identify the communication networks requiring protections~~ determine Sensitive BES Data transmitted between Control Centers requiring protections;

1.2 Procedure(s) for defining the boundaries of Communication ~~networks~~Links transmitting Sensitive BES Data ~~required for reliable operation identified~~determined in 1.1, if applicable;

1.3 Method(s) for protecting the confidentiality and integrity of data transmitted via these Communication ~~networks~~Links between Control Centers as ~~identified~~determined in 1.1, ~~where technically feasible.~~ via one or more of the following methods per Communication Link capability:

1.3.1 Encryption of the data prior to leaving the ESP or at the boundaries identified in 1.2, with decryption occurring at the boundary that the receiving Control Center has identified in 1.2.

1.3.2 Monitoring the status of the Communication Links and issuing an alarm or alert in response to detected communication failures or potential compromises to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection.

1.3.3 Implementation of an equally effective logical protection.

Additional comments received from Nathan Mitchell of APPA

Questions

1. The SDT asserts that the referenced data is already afforded protections at rest under existing CIP standards (CIP-003, 005, 007, etc.), is perishable, and has a diminished need for protection over time. Do you agree with the SDT's assertion? If you agree, please supply a rationale to support the position.

   ☒ Yes

   ☐ No

   Comments:

   The referenced data while at rest is covered in the cited Standards. Consider that real-time SCADA data performance may be impacted by disk encryption.

2. If you do not agree with the SDT's assertion in Question 1, please identify the type of data, the risk posed at rest, and supply the rationale to support the position.

   Comments:

   No comment to this question

3. Future enforceable Reliability Standards IRO-010-2 and TOP-003-3 identify "data required for reliable operation." For example, Requirement R1 of IRO-010-2 states:

R1. The Reliability Coordinator shall maintain a documented specification for the data necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments. The data specification shall include but not be limited to:

1.2. A list of data and information needed by the Reliability Coordinator to support its Operational Planning Analyses, Real-time monitoring, and Realtime Assessments including non-BES data and external network data, as deemed necessary by the Reliability Coordinator.

TOP-003-3 Requirements R1 & R2 also have similar requirements for BAs and TOPs.

Do you agree that outlining this approach for identifying "data required for reliable operation" in the Guidelines and Technical Basis is sufficient; consequently, an additional definition of "sensitive BES data" or a requirement to identify "sensitive BES data" is not necessary? If not, please explain.

☒ Yes

☐ No

Comments:

We agree with the basic approach of using TOP-003 and IRO-010 Standards to identify this data but needs to be limited to real time data. We believe TOP-003 and IRO-010 include data that is not “real time” so would be outside this document’s scope. An example of data which is out of scope includes data used for Operational Planning Analyses.

4. The SDT asserts that “availability” of inter-and intra-entity Control Center communication of data is being addressed in Project 2016-01 Modifications to TOP and IRO Standards, specifically Reliability Standards TOP-001-4 and IRO-002-5. The proposed standards require redundant and diversely routed data exchange capabilities at a Responsible Entity’s primary Control Center. Do you agree that “availability” is adequately addressed by these standards? If not, please provide rationale to support your position.

☒ Yes

☐ No

Comments:

Availability is adequately covered by other standards.

5. The SDT is proposing to develop a new CIP standard because the directives of FERC Order 822 related to the protection of communication networks used to exchange sensitive BES data regardless of the entity’s size or impact level. Do you agree with the drafting of a new CIP standard to address this issue? If you disagree and would prefer to include requirements in existing CIP Standards, such as CIP-003 and CIP-005, please provide rationale and propose requirement language.

☒ Yes

☐ No

Comments:

There are concerns about the applicability section and how it will interact with the existing CIP Standards exemption 4.2.3.2. The

applicability section should limit the scope to only real time communication networks or data between Control Centers.

Would like additional guidance on the applicability of technologies like voice communication email, text messaging …

Consider including language for CIP Exceptional Circumstances

6. The SDT evaluated multiple approaches to addressing the directive. The approach proposed in this informal posting focuses on the protection of communication links. An alternative approach could focus on the protection of the sensitive BES data itself. Do you agree with the SDT's approach to focus the draft language on the protection of communication links? If not, please provide rationale and propose alternative language.

   ☐ Yes

   ☒ No

   Comments:

   We like the option to protect either the data or the links. We would like to see these options clearly defined within the requirements and not just in the guidance. The Standard should be an outcome based Standard.

   FERC Order 822 section 58 clarifies this scope as inter-Control Center and intra-Control Center communications. The guidance seems to extend the scope beyond this by including references to DP's and listing Data links without reference to Control Centers.

7. Do you agree with the security objective of the draft language? If not, please propose alternative language.

   ☐ Yes

   ☒ No

   Comments:

   We suggest "reliability and availability" replace "confidentiality and integrity" because EMS/SCADA systems are built on "reliability and availability".

8. Is it clear what types of plans, procedures, and methods are needed to meet the draft language? If not, please propose alternative language.

   ☐ Yes

   ☒ No

   Comments:

We like the option to protect either the data or the links. We would like to see these options clearly defined within the requirements and not just in the guidance. Replace “communication networks” with “communication networks or BES reliability data”. Include in 1.1 that this is for networks or data between Control Centers.

9. The SDT uses the term “communication networks” throughout the draft language including an obligation to define the boundaries of such communication networks. Does the SDT need to define the term for inclusion in the NERC Glossary of Terms? If so, please propose a definition of “communication networks.”

☐ Yes

☒ No

Comments:

Recommend a NO vote on defining “communication network”

But consider that the FERC Order Section 58 clarifies the focus and the scope on inter-Control Center and intra-Control Center communications

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the first draft of the proposed standard.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23 - April 21, 2016
SAR posted for comment	June 1 – June 30, 2016
Informal comment period	February 10- March 13, 2017

Anticipated Actions	Date
45-day formal comment period with additional ballot	TBD
10-day final ballot	TBD
Board	TBD

Upon Board adoption, the rationale boxes will be moved to the Supplemental Material Section.

A. Introduction

1. **Title:** Cyber Security – Control Center Communication Networks
2. **Number:** CIP-012-1
3. **Purpose:** To protect confidentiality and integrity of data transmitted between Control Centers required for reliable operation of the Bulk Electric System (BES).
4. **Applicability:**
   - **4.1. Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.
     - **4.1.1. Balancing Authority**
     - **4.1.2. Generator Operator**
     - **4.1.3. Generator Owner**
     - **4.1.4. Reliability Coordinator**
     - **4.1.5. Transmission Operator**
     - **4.1.6. Transmission Owner**
   - 4.2. **Exemptions:** The following are exempt from Reliability Standard CIP-012-1:
     - **4.2.1.** Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.
     - **4.2.2.** The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.
5. **Effective Date:** See Implementation Plan for CIP-012-1

B. Requirements and Measures

Rationale for Requirements R1 and R2: FERC Order No. 822 directed NERC to develop modifications to the CIP Reliability Standards to require Responsible Entities to implement controls to protect communication links and sensitive Bulk Electric System (BES) data communicated between BES Control Centers. Reliability Standard CIP-012-1 responds to that directive, requiring Responsible Entities to develop a plan to protect the confidentiality and integrity of sensitive data while being transmitted between Control Centers. Responsible Entities use various means to communicate information between

Control Centers. The plan for protecting these communications is required for all impact levels due to the inter-dependency of multiple impact levels.

The type of data in scope of CIP-012-1 is data used for Operational Planning Analyses, Real-time Assessments, and Real-time monitoring. The terms Operational Planning Analyses, Real-time Assessments, and Real-time used are defined in the Glossary of Terms Used in NERC Reliability Standards and used in TOP-003 and IRO-010, among other Reliability Standards.

There are differences between the plan(s) required to be developed and implemented for CIP-012-1 and the protection required in CIP-006-6 Requirement R1 Part 1.10. CIP-012-1 Requirements R1 and R2 protect the applicable data during transmission between two geographically separate Control Centers. CIP-006 Requirement R1 Part 1.10 protects nonprogrammable communication components within an Electronic Security Perimeter (ESP) but outside of a Physical Security Perimeter (PSP). The transmission of applicable data between Control Centers takes place outside of an ESP. Therefore, the protection contained in CIP-006-6 Requirement R1 Part 1.10 does not apply.

R1. The Responsible Entity shall develop one or more documented plan(s) to mitigate the risk of the unauthorized disclosure or modification of data used for Operational Planning Analysis, Real-time Assessments, and Real-time monitoring while being transmitted between Control Centers. This excludes oral communications. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. Risk mitigation shall be accomplished by one or more of the following actions:

- Physically protecting the communication links transmitting the data;
- Logically protecting the data during transmission; or
- Using an equally effective method to mitigate the risk of unauthorized disclosure or modification of the data.

Note: If the Responsible Entity does not have a Control Center or it does not transmit the type of data specified in Requirement R1 of CIP-012-1 between two Control Centers, the requirements in CIP-012-1 would not apply to that entity.

M1. Evidence may include, but is not limited to, documented plan(s) that meet the security objective of Requirement R1.

R2. The Responsible Entity shall implement the plan(s) specified in Requirement R1, except under CIP Exceptional Circumstances.

M2. Evidence may include, but is not limited to, documentation to demonstrate implementation of methods to mitigate the risk of the unauthorized disclosure or modification of data in Requirement R1.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

- The Responsible Entities shall keep data or evidence of each Requirement in this Reliability Standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The Compliance Enforcement Authority (CEA) shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	N/A	N/A	N/A	The Responsible Entity failed to document one or more plan(s) that achieve the security objective to mitigate the risk of unauthorized disclosure or modification of data used for Operational Planning Analysis, Real-time Assessments, and Real-time monitoring while being transmitted, excluding oral communication, between Control Centers as specified in Requirement R1.
R2.	N/A	N/A	N/A	The Responsible Entity failed to implement its plan(s) to mitigate the risk of unauthorized disclosure or modification of data used for Operational Planning Analysis, Real-time Assessments, and Real-time

				monitoring while being transmitted, excluding oral communication, between Control Centers as specified in Requirement R1, except under CIP Exceptional Circumstances.

D. Regional Variances

None.

E. Associated Documents

Implementation Plan.

Version History

Version	Date	Action	Change Tracking
1	TBD	Respond to FERC Order No. 822	N/A

Standard Attachments

None.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2016-02 Modifications to CIP Standards
Reliability Standard CIP-012-1

Applicable Standard

- Reliability Standard CIP-012-1 - Cyber Security – Control Center Communication Networks

Requested Retirements

- None

Prerequisite Standard

These standard(s) or definitions must be approved before the Applicable Standard becomes effective:

- None

Applicable Entities

- Balancing Authority
- Generator Operator
- Generator Owner
- Reliability Coordinator
- Transmission Operator
- Transmission Owner

Effective Date

Reliability Standard CIP-012-1 - Cyber Security – Control Center Communication Networks

Where approval by an applicable governmental authority is required, Reliability Standard CIP-012-1 shall become effective on the first day of the first calendar quarter that is twelve (12) calendar months after the effective date of the applicable governmental authority's order approving the standard, or as otherwise provided for by the applicable governmental authority.

Where approval by an applicable governmental authority is not required, Reliability Standard CIP-012-1 shall become effective on the first day of the first calendar quarter that is twelve (12) calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Comment Form

Project 2016-02 Modifications to CIP Standards
CIP-012-1

Do not use this form for submitting comments. Use the electronic form to submit comments on **CIP-012-1 - Cyber Security – Control Center Communication Networks.** The electronic form must be submitted by **8 p.m. Eastern, Monday, September 11, 2017.**

Additional information is available on the project page. If you have questions, contact Standards Developers, Katherine Street (404-446-69702) or Mat Bunch (404-446-9785).

Background Information

On January 21, 2016, the Commission issued Order No. 822, approving seven CIP Reliability Standards and new or modified definitions, and directing modifications to the CIP Reliability Standards. Among others, the Commission directed NERC to "develop modifications to the CIP Reliability Standards to require responsible entities to implement controls to protect, at a minimum, communication links and sensitive bulk electric system data communicated between bulk electric system Control Centers in a manner that is appropriately tailored to address the risks posed to the bulk electric system by the assets being protected (i.e., high, medium, or low impact)." (Order 822, Paragraph 53)

The Project 2016-02 Standard Drafting Team (SDT) drafted Reliability Standard CIP-012-1 to require Responsible Entities to implement controls to protect sensitive Bulk Electric System (BES) data and communications links between BES Control Centers. Due to the sensitivity of the data being communicated between the Control Centers, as defined in the NERC Glossary of Terms Used in Reliability Standards, the standard applies to all impact levels (i.e., high, medium, or low impact).

The SDT drafted requirements allowing Responsible Entities to apply protection to the links, the data, or both, to satisfy the security objective consistent with the capabilities of the Responsible Entity's operational environment. Requirement R1 requires Responsible Entities to document one or more plans that protect Operational Planning Analysis, Real-time Assessment, and Real-time monitoring data while being transmitted between Control Centers. The plan(s) must address how the Responsible Entity will mitigate the risk of unauthorized disclosure or modification of the applicable data. Requirement R2 covers implementation of the plan developed according to Requirement R1.

Questions

1. Requirement R1: The SDT drafted CIP-012-1 Requirement R1 to meet the mandatory requirement for the Responsible Entity to develop one or more documented plan(s) to mitigate the risk of the unauthorized disclosure or modification of data used for Operational Planning Analysis, Real-time Assessment, and Real-time monitoring data while being transmitted between Control Centers. Do you agree with this revision? If not, please provide the basis for your disagreement and an alternate proposal.

   ☐ Yes
   ☐ No
   Comments:

2. Requirement R1: The SDT seeks comment on the need to scope sensitive BES data as it applies to Operational Planning Analysis, Real-time Assessment, and Real-time monitoring. Do you agree with scoping CIP-012-1 Requirement R1 in this manner? Please provide comment in support of your response.

   ☐ Yes
   ☐ No
   Comments:

3. Implementation Plan: The SDT revised the Implementation Plan such that the standard and NERC Glossary terms are effective the first day of the first calendar quarter that is twelve (12) calendar months after the effective date of the applicable governmental authority's order approving the standard, or as otherwise provided for by the applicable governmental authority. Do you agree with this proposal? If you agree with the proposed implementation time period, please note the actions you will take that require this amount of time to complete. If you think an alternate implementation time period is needed – shorter or longer - please propose an alternate implementation plan and provide a detailed explanation of actions and time needed to meet the implementation deadline.

   ☐ Yes
   ☐ No
   Comments:

4. The SDT believes proposed CIP-012-1 provides entities with flexibility to meet the reliability objectives in a cost effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost effective approaches, please provide your recommendation and, if appropriate, technical justification.

   ☐ Yes
   ☐ No
   Comments:

5. If you have additional comments on the proposed CIP-012-1 – Cyber Security -- Communication Networks drafted in response to the FERC directive that you have **not** provided in response to the questions above, please provide them here.

   Comments:

Project 2016-02 Consideration of Issues and Directives

Federal Energy Regulatory Commission Order No. 822

June 21, 2017

Directives from Order 822		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
53	53. As discussed in detail below, however, the Commission concludes that modifications to CIP-006-6 to provide controls to protect, at a minimum, communication links and data communicated between bulk electric system Control Centers are necessary in light of the critical role Control Center communications play in maintaining bulk electric system reliability. Therefore, we adopt the NOPR proposal and direct that NERC, pursuant to section 215(d)(5) of the FPA, develop modifications to the CIP Reliability Standards to require responsible entities to implement controls to protect, at a minimum, communication links and sensitive bulk electric system data communicated between bulk electric system Control Centers in a manner that is appropriately tailored to address the risks posed to the bulk electric system by the assets being protected (i.e., high, medium, or low impact).	The Project 2016-02 Standard Drafting Team (SDT) drafted Reliability Standard CIP-012-1 Requirement R1 to require responsible entities to document one or more plan(s) to mitigate the risk of the unauthorized disclosure or modification of data used for Operational Planning Analysis, Real-time Assessments, and Real-time monitoring while being transmitted between Bulk Electric System (BES) Control Centers. Requirement R2 requires implementation of the documented plan(s). Due to the sensitivity of the data being transmitted between the Control Centers, as defined in the NERC Glossary of Terms Used in Reliability Standards, the SDT created the standard and determined that it applies to all impact levels of BES Cyber Systems (i.e., high, medium, or low impact). The SDT has drafted requirements allowing Responsible Entities to apply protection to the links, the data, or both, to satisfy the security objective of the Commission's directive, consistent with the capabilities of the Responsible Entity's

Directives from Order 822		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
		operational environment. The directive language specifically references CIP-006-6 which pertains to physical security controls. CIP-006-6, Requirement R1, Part 1.10 focuses on protecting the nonprogrammable communication components between Cyber Assets within the same ESP for medium and high impact BES Cyber Systems. The SDT asserts that most of the communications contemplated by the Order are not within the same ESP, and that CIP-006-6, Requirement R1, Part 1.10 would not be the appropriate location for this requirement.
54	54. NERC and other commenters recognize that inter-Control Center communications play a critical role in maintaining bulk electric system reliability by, among other things, helping to maintain situational awareness and reliable bulk electric system operations through timely and accurate communication between Control Centers.[59] We agree with this assessment. In order for certain responsible entities such as reliability coordinators, balancing authorities, and transmission operators to adequately perform their reliability functions, their associated control centers must be capable of receiving and storing a variety of sensitive bulk electric system data from interconnected entities. Accordingly, we find that additional measures to protect both the integrity and availability of sensitive bulk	The SDT agrees that inter-Control Center communications play a critical role in Bulk Electric System reliability. Responsible Entities should therefore apply security measures to mitigate the risk of the unauthorized disclosure or modification of data used for Operational Planning Analysis, Real-time Assessments, and Real-time monitoring, which the current CIP Reliability Standards do not address. As such, the SDT has defined requirements that are designed to protect the data while it is being transmitted between inter-entity and intra-entity Control Centers. The SDT has drafted requirements allowing responsible entities to apply protection to the links, the data, or both to satisfy the security objective consistent with the capabilities of the responsible entity's operational environment.

Directives from Order 822		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
	electric system data are warranted.[60] We also understand that the attributes of the data managed by responsible entities could require different information protection controls. [61] For instance, certain types of reliability data will be sensitive to data manipulation type attacks, while other types of reliability data will be sensitive to eavesdropping type attacks aimed at collecting operational information (such as line and equipment ratings and impedances). NERC should consider the differing attributes of bulk electric system data as it assesses the development of appropriate controls. Footnotes: [59] NERC Comments at 20. [60] Protecting the integrity of bulk electric system data involves maintaining and ensuring the accuracy and consistency of inter-Control Center communications. Protecting the availability of bulk electric system data involves ensuring that required data is available when needed for bulk electric system operations. [61] Moreover, in order for certain responsible entities to adequately perform their Reliability Functions, the associated control centers must be capable of receiving and storing a variety of sensitive data as specified by the	

Directives from Order 822		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
	IRO and TOP Standards. For instance, pursuant to Reliability Standard TOP-003-3, Requirements R1, R3 and R5, a transmission operator must maintain a documented specification for data and distribute its data specification to entities that have data required by the transmission operator's Operational Planning Analyses, Real-time Monitoring and Real-time Assessments. Entities receiving a data specification must satisfy the obligation of the documented specification.	
55	55. With regard to NERC's development of modifications responsive to our directive, we agree with NERC and other commenters that NERC should have flexibility in the manner in which it addresses the Commission's directive. Likewise, we find reasonable the principles outlined by NERC that protections for communication links and sensitive bulk electric system data communicated between bulk electric system Control Centers: (1) should not have an adverse effect on reliability, including the recognition of instances where the introduction of latency could have negative results; (2) should account for the risk levels of assets and information being protected, and require protections that are commensurate with the risks presented; and (3) should be results-based in order to provide flexibility to	The SDT drafted Reliability Standard CIP-012-1 to establish requirements to mitigate the risk of the unauthorized disclosure or modification of data used for Operational Planning Analysis, Real-time Assessments, and Real-time monitoring while being transmitted between Control Centers. The SDT developed objective-based rather than prescriptive requirements. This approach will allow Responsible Entities flexibility in protecting these communications networks and sensitive BES data in a manner suited to each of their respective environments. It will also allow Responsible Entities to implement protection that considers the risks noted by the Commission. The SDT identified a need to mitigate the risk of the unauthorized disclosure or modification of data used for Operational Planning Analysis, Real-time Assessment, and Real-time monitoring regardless of asset risk level. The proposal requires protection for all data used for Operational Planning Analysis, Real-time Assessment, and Real-

Directives from Order 822		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
	account for the range of technologies and entities involved in bulk electric system communications.[62] Footnote: [62] See NERC Comments at 20-21.	time monitoring while being transmitted between Control Centers.
56	56. We disagree with the assertion of NIPSCO and G&T Cooperatives that the risk posed by bulk electric system communication networks does not justify the costs of implementing controls. Communications between Control Centers over such networks are fundamental to the operations of the bulk electric system, and the record here does not persuade us that controls for such networks are not available at a reasonable cost (through encryption or otherwise). Nonetheless, we recognize that not all communication network components and data pose the same risk to bulk electric system reliability and may not require the same level of protection. We expect NERC to develop controls that reflect the risk posed by the asset or data being protected, and that can be implemented in a reasonable manner. It is important to recognize that certain entities are already required to exchange necessary real-time and operational planning data through secured networks using a "mutually agreeable security protocol," regardless of the entity's	The SDT noted the FERC reference to additional Reliability Standards and the responsibilities to protect the data in accordance with those standards (TOP-003-3 and IRO-010-2). The SDT interpreted these references as examples of potentially sensitive BES data and chose to base the CIP-012 requirements on the data specifications in these standards. This consolidates scoping and helps ensure that Responsible Entities mitigate the risk of the unauthorized disclosure or modification of Operational Planning Analysis, Real-time Assessment, and Real-time monitoring data, rather than leaving the scoping to individual Responsible Entities. The SDT drafted CIP-012-1 to address confidentiality and integrity of data used for Operational Planning Analysis, Real-time Assessment, and Real-time monitoring. These are accommodated by drafting the requirement to mitigate the risk from unauthorized disclosure or modification. The SDT contends that the availability of this data is already required by the performance obligation of the Operating and Planning Reliability Standards.

Directives from Order 822		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
	size or impact level.[63] 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. Footnote: [63] See Reliability Standards TOP-003-3, Requirement R5 and IRO-010-2, Requirement R3.	The SDT drafted CIP-012-1 to address the data while being transmitted. The SDT contends that this data is maintained within BES Cyber Systems, and is afforded the protections of CIP-003 through CIP-011.
58	58. Several commenters sought clarification whether Control Centers owned by multiple registered entities would be included under the Commission's proposal. We clarify that the scope of the directed modifications apply to Control Center communications from facilities at all impact levels, regardless of ownership. The directed modification should encompass communication links and data for intra-Control Center and inter-Control Center communications.	The SDT created the standard and determined that it applies to all impact levels of BES Cyber Systems (i.e., high, medium, or low impact), regardless of ownership. The SDT defined requirements that are designed to mitigate the risk of the unauthorized disclosure or modification of data used for Operational Planning Analysis, Real-time Assessment, and Real-time monitoring while being transmitted between inter-entity and intra-entity BES Control Centers.
62	62. Several commenters addressed encryption and latency. Based on the record in this proceeding, it is reasonable to conclude that any lag in communication speed resulting from implementation of protections should only be measureable on the order of	The SDT developed objective-based rather than prescriptive requirements. This approach will allow Responsible Entities flexibility in mitigating the risk of the unauthorized disclosure or modification of data used for Operational Planning Analysis,

Directives from Order 822		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
	milliseconds and, therefore, will not adversely impact Control Center communications. Several commenters raise possible technical implementation difficulties with integrating encryption technologies into their current communications networks. Such technical issues should be considered by the standard drafting team when developing modifications in response to this directive, and may be resolved, e.g., by making certain aspects of the revised CIP Standards eligible for Technical Feasibility Exceptions.	Real-time Assessments, and Real-time monitoring in a manner suited to each of their respective environments. It will also allow Responsible Entities to implement protection that considers the risks noted by the Commission.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Violation Risk Factor and Violation Severity Level Justifications

Project 2016-02 Modifications to CIP Standards

This document provides the standard drafting team's (SDT's) justification for assignment of violation risk factors (VRFs) and violation severity levels (VSLs) for each requirement in **CIP-012-1**. Each requirement is assigned a VRF and a VSL. These elements support the determination of an initial value range for the Base Penalty Amount regarding violations of requirements in FERC-approved Reliability Standards, as defined in the Electric Reliability Organizations (ERO) Sanction Guidelines. The SDT applied the following NERC criteria and FERC Guidelines when developing the VRFs and VSLs for the requirements.

NERC Criteria for Violation Risk Factors

High Risk Requirement

A requirement that, if violated, could directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures, or could hinder restoration to a normal condition.

Medium Risk Requirement

A requirement that, if violated, could directly affect the electrical state or the capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System. However, violation of a medium risk requirement is unlikely to lead to Bulk Electric System instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System. However, violation of a medium risk requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to Bulk Electric System instability, separation, or cascading failures, nor to hinder restoration to a normal condition.

Lower Risk Requirement
A requirement that is administrative in nature and a requirement that, if violated, would not be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System; or, a requirement that is administrative in nature and a requirement in a planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.

FERC Guidelines for Violation Risk Factors

Guideline (1) – Consistency with the Conclusions of the Final Blackout Report

FERC seeks to ensure that VRFs assigned to Requirements of Reliability Standards in these identified areas appropriately reflect their historical critical impact on the reliability of the Bulk-Power System. In the VSL Order, FERC listed critical areas (from the Final Blackout Report) where violations could severely affect the reliability of the Bulk-Power System:

- Emergency operations
- Vegetation management
- Operator personnel training
- Protection systems and their coordination
- Operating tools and backup facilities
- Reactive power and voltage control
- System modeling and data exchange
- Communication protocol and facilities
- Requirements to determine equipment ratings
- Synchronized data recorders
- Clearer criteria for operationally critical facilities
- Appropriate use of transmission loading relief.

Guideline (2) – Consistency within a Reliability Standard

FERC expects a rational connection between the sub-Requirement VRF assignments and the main Requirement VRF assignment.

Guideline (3) – Consistency among Reliability Standards

FERC expects the assignment of VRFs corresponding to Requirements that address similar reliability goals in different Reliability Standards would be treated comparably.

Guideline (4) – Consistency with NERC's Definition of the Violation Risk Factor Level

Guideline (4) was developed to evaluate whether the assignment of a particular VRF level conforms to NERC's definition of that risk level.

Guideline (5) – Treatment of Requirements that Co-mingle More Than One Obligation

Where a single Requirement co-mingles a higher risk reliability objective and a lesser risk reliability objective, the VRF assignment for such Requirements must not be watered down to reflect the lower risk level associated with the less important objective of the Reliability Standard.

NERC Criteria for Violation Severity Levels

VSLs define the degree to which compliance with a requirement was not achieved. Each requirement must have at least one VSL. While it is preferable to have four VSLs for each requirement, some requirements do not have multiple "degrees" of noncompliant performance and may have only one, two, or three VSLs.

VSLs should be based on NERC's overarching criteria shown in the table below:

Lower VSL	Moderate VSL	High VSL	Severe VSL
The performance or product measured almost meets the full intent of the requirement.	The performance or product measured meets the majority of the intent of the requirement.	The performance or product measured does not meet the majority of the intent of the requirement, but does meet some of the intent.	The performance or product measured does not substantively meet the intent of the requirement.

FERC Order of Violation Severity Levels

The FERC VSL guidelines are presented below, followed by an analysis of whether the VSLs proposed for each requirement in the standard meet the FERC Guidelines for assessing VSLs:

Guideline (1) – Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance

Compare the VSLs to any prior levels of non-compliance and avoid significant changes that may encourage a lower level of compliance than was required when levels of non-compliance were used.

Guideline (2) – Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties

A violation of a "binary" type requirement must be a "Severe" VSL.

Do not use ambiguous terms such as "minor" and "significant" to describe noncompliant performance.

Guideline (3) – Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement

VSLs should not expand on what is required in the requirement.

Guideline (4) – Violation Severity Level Assignment Should Be Based on a Single Violation, Not on a Cumulative Number of Violations

Unless otherwise stated in the requirement, each instance of non-compliance with a requirement is a separate violation. Section 4 of the Sanction Guidelines states that assessing penalties on a per violation per day basis is the "default" for penalty calculations.

VRF Justifications for CIP-012-1, Requirement R1	
Proposed VRF	**Medium**
NERC VRF Discussion	A VRF of Medium was assigned to this requirement. Cyber security plans enable effective implementation of the CIP standard's requirements to mitigate the risk of the unauthorized disclosure or modification of data used for Operational Planning Analysis, Real-time Assessments, and Real-time monitoring while being transmitted between Control Centers.
FERC VRF G1 Discussion Guideline 1- Consistency with Blackout Report	N/A
FERC VRF G2 Discussion Guideline 2- Consistency within a Reliability Standard	N/A
FERC VRF G3 Discussion Guideline 3- Consistency among Reliability Standards	The requirement complements CIP-005-1, Requirement R1, CIP-006-6, Requirement R1, and CIP-007-6, Requirement R1 which are related to security of networks and communications components. The proposed VRF is consistent with these related requirements.
FERC VRF G4 Discussion Guideline 4- Consistency with NERC Definitions of VRFs	Failure to have a cyber security plan would not, under Emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.
FERC VRF G5 Discussion	N/A

VRF Justifications for CIP-012-1, Requirement R1	
Proposed VRF	**Medium**
Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation	

VSLs for CIP-012-1, Requirement R1			
Lower	**Moderate**	**High**	**Severe**
N/A	N/A	N/A	The Responsible Entity failed to document one or more plan(s) that achieve the security objective to mitigate the risk of the unauthorized disclosure or modification of data used for Operational Planning Analysis, Real-time Assessments, and Real-time monitoring while being transmitted, excluding oral communication, between Controls Centers as specified in Requirement R1.

VSL Justifications for CIP-012-1 Requirements R1	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The requirement is new. Therefore, the proposed VSL does not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSL is binary and is classified as severe. The VSL does not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL uses the same terminology as used in the associated requirement and is, therefore, consistent with the requirement.

FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSL is based on a single violation and not cumulative violations.

VRF Justifications for CIP-012-1, Requirement R2	
Proposed VRF	**Medium**
NERC VRF Discussion	A VRF of Medium was assigned to this requirement. Implementation of required cyber security plans enable effective implementation of the CIP standard's requirements to mitigate the risk of the unauthorized disclosure or modification of data used for Operational Planning Analysis, Real-time Assessments, and Real-time monitoring while being transmitted between Control Centers.
FERC VRF G1 Discussion Guideline 1- Consistency with Blackout Report	N/A
FERC VRF G2 Discussion Guideline 2- Consistency within a Reliability Standard	N/A
FERC VRF G3 Discussion Guideline 3- Consistency among Reliability Standards	The requirement complements CIP-005-1, Requirement R1, CIP-006-6, Requirement R1, and CIP-007-6, Requirement R1 which are related to security of networks and communications components. The proposed VRF is consistent with these related requirements.
FERC VRF G4 Discussion	Failure to properly implement the cyber security plan would not, under Emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state

VRF Justifications for CIP-012-1, Requirement R2	
Proposed VRF	**Medium**
Guideline 4- Consistency with NERC Definitions of VRFs	or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.
FERC VRF G5 Discussion Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation	N/A

VSLs for CIP-012-1, Requirement R2			
Lower	**Moderate**	**High**	**Severe**
N/A	N/A	N/A	The Responsible Entity failed to implement its plan to mitigate the risk of the unauthorized disclosure or modification of data used for Operational, Planning Analysis, Real-time Assessments, and Real-time monitoring while being transmitted, excluding oral communication, between Controls Centers as specified in Requirement R1, except under CIP Exceptional Circumstances.

VSL Justifications for CIP-012-1 Requirement R2	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The requirement is new. Therefore, the proposed VSL does not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSL is binary and is classified as severe. The VSL does not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL uses the same terminology as used in the associated requirement and is, therefore, consistent with the requirement.

FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSL is based on a single violation and not cumulative violations.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Reliability Standard Audit Worksheet[1]

CIP-012-1 – Cyber Security – Control Center Communication Networks

This section to be completed by the Compliance Enforcement Authority.

Audit ID:	Audit ID if available; or REG-NCRnnnnn-YYYYMMDD
Registered Entity:	Registered name of entity being audited
NCR Number:	NCRnnnnn
Compliance Enforcement Authority:	Region or NERC performing audit
Compliance Assessment Date(s)[2]:	Month DD, YYYY, to Month DD, YYYY
Compliance Monitoring Method:	[On-site Audit | Off-site Audit | Spot Check]
Names of Auditors:	Supplied by CEA

Applicability of Requirements

	BA	DP	GO	GOP	PA/PC	RC	RP	RSG	TO	TOP	TP	TSP
R1	X		X	X		X			X	X		
R2	X		X	X		X			X	X		

Legend:

Text with blue background:	Fixed text – do not edit
Text entry area with Green background:	Entity-supplied information
Text entry area with white background:	Auditor-supplied information

[1] NERC developed this Reliability Standard Audit Worksheet (RSAW) language in order to facilitate NERC's and the Regional Entities' assessment of a registered entity's compliance with this Reliability Standard. The NERC RSAW language is written to specific versions of each NERC Reliability Standard. Entities using this RSAW should choose the version of the RSAW applicable to the Reliability Standard being assessed. While the information included in this RSAW provides some of the methodology that NERC has elected to use to assess compliance with the requirements of the Reliability Standard, this document should not be treated as a substitute for the Reliability Standard or viewed as additional Reliability Standard requirements. In all cases, the Regional Entity should rely on the language contained in the Reliability Standard itself, and not on the language contained in this RSAW, to determine compliance with the Reliability Standard. NERC's Reliability Standards can be found on NERC's website. Additionally, NERC Reliability Standards are updated frequently, and this RSAW may not necessarily be updated with the same frequency. Therefore, it is imperative that entities treat this RSAW as a reference document only, and not as a substitute or replacement for the Reliability Standard. It is the responsibility of the registered entity to verify its compliance with the latest approved version of the Reliability Standards, by the applicable governmental authority, relevant to its registration status.

The RSAW may provide a non-exclusive list, for informational purposes only, of examples of the types of evidence a registered entity may produce or may be asked to produce to demonstrate compliance with the Reliability Standard. A registered entity's adherence to the examples contained within this RSAW does not necessarily constitute compliance with the applicable Reliability Standard, and NERC and the Regional Entity using this RSAW reserve the right to request additional evidence from the registered entity that is not included in this RSAW. This RSAW may include excerpts from FERC Orders and other regulatory referenceswhich are provided for ease of reference only, and this document does not necessarily include all applicable Order provisions. In the event of a discrepancy between FERC Orders, and the language included in this document, FERC Orders shall prevail.

[2] Compliance Assessment Date(s): The date(s) the actual compliance assessment (on-site audit, off-site spot check, etc.) occurs.

Findings

(This section to be completed by the Compliance Enforcement Authority)

Req.	Finding	Summary and Documentation	Functions Monitored
R1			
R2			

Req.	Areas of Concern

Req.	Recommendations

Req.	Positive Observations

Subject Matter Experts

Identify the Subject Matter Expert(s) responsible for this Reliability Standard.

Registered Entity Response (Required; Insert additional rows if needed):

SME Name	Title	Organization	Requirement(s)

Registered Entity Response (Required):
Question 1: Does the Registered Entity own or operate a Control Center? ☐ Yes ☐ No

If no:

1. Provide evidence in the space that the Registered Entity does not own or operate one or more Control Centers. This evidence may include, but is not limited to:
   - Evidence that the Registered Entity does not own or operate a Control Center; or
   - Evidence that the Registered Entity's asset list does not contain a Control Center.
2. The remainder of this RSAW may be left blank.

If yes, continue with Question 2.

[Note: A separate spreadsheet or other document may be used. If so, provide the document reference below.]

Question 2: Is data used for Operational Planning Analysis, Real-time Assessments, or Real-time monitoring transmitted between Control Centers at any time by any Control Center owned or operated by the Registered Entity? ☐ Yes ☐ No

If no:

1. Provide evidence in the space below supporting this assertion. This evidence may include, but is not limited to:
   - Evidence demonstrating data used for Operational Planning Analysis, Real-time Assessments, and Real-time monitoring is not transmitted between Control Centers at any time by any Control Center owned or operated by the Registered Entity.
2. The remainder of this RSAW may be left blank.

If yes, continue with the remainder of this RSAW.

[Note: A separate spreadsheet or other document may be used. If so, provide the document reference below.]

R1 Supporting Evidence and Documentation

R1. The Responsible Entity shall develop one or more documented plan(s) to mitigate the risk of the unauthorized disclosure or modification of data used for Operational Planning Analysis, Real-time Assessments, and Real-time monitoring while being transmitted between Control Centers. This excludes oral communications. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1 Risk mitigation shall be accomplished by one or more of the following actions:

- Physically protecting the communication links transmitting the data;
- Logically protecting the data during transmission; or
- Using an equally effective method to mitigate the risk of unauthorized disclosure or modification of the data.

Note: If the Responsible Entity does not have a Control Center or it does not transmit the type of data specified in Requirement R1 of CIP-012-1 between two Control Centers, the requirements in CIP-012-1 would not apply to that entity.

M1. Evidence may include, but is not limited to, documented plan(s) that meet the security objective of Requirement R1.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-012-1, R1

This section to be completed by the Compliance Enforcement Authority

	If the Registered Entity has answered "No" to either Question 1 or Question 2, verify: • The Registered Entity does not own or operate a Control Center; or • The Registered Entity does not transmit data used for Operational Planning Analysis, Real-time Assessments, or Real-time monitoring at any time between Control Centers.
	If the Registered Entity has answered "Yes" to Question 2, verify: 1. The entity has developed one or more documented plans to mitigate the risk of the unauthorized disclosure or modification of data used for Operational Planning Analysis, Real-time Assessments, and Real-time monitoring while being transmitted between Control Centers; 2. The documented plan(s) collectively address all data used for Operational Planning Analysis, Real-time Assessments, and Real-time monitoring transmitted between Control Centers; and 3. The documented plan(s) collectively accomplish risk mitigation by one or more of the following actions: • Physically protecting the communication links transmitting the data; • Logically protecting the data during transmission; or • Using an equally effective method to mitigate the risk of unauthorized disclosure or modification of the data.
Note to Auditor: 1. Oral communications are not in scope for CIP-012-1.	

Auditor Notes:

R2 Supporting Evidence and Documentation

R2. The Responsible Entity shall implement the plan(s) specified in Requirement R1, except under CIP Exceptional Circumstances.

M2. Evidence may include, but is not limited to, documentation to demonstrate implementation of methods to mitigate the risk of the unauthorized disclosure or modification of data in Requirement R1.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-012-1, R2

This section to be completed by the Compliance Enforcement Authority

	If the Registered Entity has answered "Yes" to Question 2, verify with system-generated evidence (where available) that the Registered Entity has implemented the plan(s) specified in Requirement R1, except under CIP Exceptional Circumstances.
	If the Responsible Entity has declared and responded to CIP Exceptional Circumstances, verify the Responsible Entity has adhered to the applicable cyber security policies.
Note to Auditor: The Responsible Entity may reference a separate set of documents to demonstrate its response to any requirements impacted by CIP Exceptional Circumstances.	

Auditor Notes:

Additional Information:

Reliability Standard

The full text of CIP-012-1 may be found on the NERC Web Site (www.nerc.com) under "Program Areas & Departments", "Reliability Standards."

In addition to the Reliability Standard, there is an applicable Implementation Plan available on the NERC Web Site.

In addition to the Reliability Standard, there is background information available on the NERC Web Site.

Capitalized terms in the Reliability Standard refer to terms in the NERC Glossary, which may be found on the NERC Web Site.

Sampling Methodology

Sampling is essential for auditing compliance with NERC Reliability Standards since it is not always possible or practical to test 100% of either the equipment, documentation, or both, associated with the full suite of enforceable standards. The Sampling Methodology Guidelines and Criteria (see NERC website), or sample guidelines, provided by the Electric Reliability Organization help to establish a minimum sample set for monitoring and enforcement uses in audits of NERC Reliability Standards.

Regulatory Language

FERC Order 822 P53-56, 58, and 62

Selected Glossary Terms

The following Glossary terms are provided for convenience only. Please refer to the NERC web site for the current enforceable terms.

CIP Exceptional Circumstance

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.

Control Center

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, of: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for transmission Facilities at two or more locations, or 4) a Generator Operator for generation Facilities at two or more locations.

Operational Planning Analysis

An evaluation of projected system conditions to assess anticipated (pre-Contingency) and potential (post-Contingency) conditions for next-day operations. The evaluation shall reflect applicable inputs including, but

not limited to, load forecasts; generation output levels; Interchange; known Protection System and Special Protection System status or degradation; Transmission outages; generator outages; Facility Ratings; and identified phase angle and equipment limitations. (Operational Planning Analysis may be provided through internal systems or through third-party services.)

Real-time Assessment

An evaluation of system conditions using Real-time data to assess existing (pre-Contingency) and potential (post-Contingency) operating conditions. The assessment shall reflect applicable inputs including, but not limited to: load, generation output levels, known Protection System and Special Protection System status or degradation, Transmission outages, generator outages, Interchange, Facility Ratings, and identified phase angle and equipment limitations. (Real-time Assessment may be provided through internal systems or through third-party services.)

Real-time

Present time as opposed to future time.

Revision History for RSAW

Version	Date	Reviewers	Revision Description
Draft1 v1	07/28/2017	NERC Stds Group	New document
Draft1 v2	08/01/2017	RSAW Task Force	Modified Question to clarify applicability
Draft1 v3	08/02/2017	RSAW Task Force	Response to MRO comments. Moved Questions 1 and 2 above R1. Made text changes to Q1 and to R2 Compliance Assessment Approach.
Draft1 v4	08/07/2017	RSAW Tasf Force, 2016-02 SDT	Response to TexasRE and SDT comments. Clarified scope of Q1 to be data transmitted between Control Centers. Removed extra space from Auditor Notes.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Reminder

Project 2016-02 Modifications to CIP Standards

Initial Ballot and Non-binding Poll Open through September 11, 2017

Now Available

An initial ballot for **CIP-012-1 - Cyber Security – Control Center Communication Networks** and non-binding poll of the associated Violation Risk Factors and Violation Severity Levels are open through **8 p.m. Eastern, Monday, September 11, 2017**

Balloting

Members of the ballot pools associated with this project can log in and submit their votes by accessing the Standards Balloting and Commenting System (SBS) here. If you experience any difficulties in navigating the SBS, contact Wendy Muller.

- *If you are having difficulty accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out, contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern).*
- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*
- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Next Steps

The ballot results will be announced and posted on the project page. The drafting team will review all responses received during the comment period and determine the next steps of the project.

For information on the Standards Development Process, refer to the Standard Processes Manual**.**

For more information or assistance, contact Standards Developers, Katherine Street at (404) 446-9702 or Mat Bunch at (404) 446-9785.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2016-02 Modifications to CIP Standards
CIP-012-1

Formal Comment Period Open through September 11, 2017
Ballot Pools Forming through August 25, 2017

Now Available

A 45-day formal comment period for **CIP-012-1 - Cyber Security – Control Center Communication Networks** is open through **8 p.m. Eastern, Monday, September 11, 2017.**

Commenting

Use the electronic form to submit comments. If you experience any difficulties using the electronic form, contact Wendy Muller. An unofficial Word version of the comment form is posted on the project page.

Ballot Pools

Ballot pools are being formed through **8 p.m. Eastern, Friday, August 25, 2017.** Registered Ballot Body members may join the ballot pools here.

If you are having difficulty accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out, contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern).

- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*
- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Next Steps

An initial ballot for the standard and non-binding poll of the associated Violation Risk Factors and Violation Severity Levels will be conducted September 1-11, 2017.

For information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, Katherine Street (via email) or at (404) 446-9702 or Mat Bunch (via email) or at (404) 446-9785.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/102)
Ballot Name: 2016-02 Modifications to CIP Standards CIP-012-1 IN 1 ST
Voting Start Date: 9/1/2017 12:01:00 AM
Voting End Date: 9/11/2017 11:59:59 PM
Ballot Type: ST
Ballot Activity: IN
Ballot Series: 1
Total # Votes: 248
Total Ballot Pool: 309
Quorum: 80.26
Weighted Segment Value: 42.74

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	80	1	24	0.393	37	0.607	0	1	18
Segment: 2	7	0.6	1	0.1	5	0.5	0	0	1
Segment: 3	73	1	24	0.429	32	0.571	0	3	14
Segment: 4	17	1	5	0.313	11	0.688	0	0	1
Segment: 5	73	1	16	0.276	42	0.724	0	2	13
Segment: 6	46	1	12	0.353	22	0.647	0	0	12
Segment: 7	2	0.1	1	0.1	0	0	0	0	1
Segment: 8	3	0.3	3	0.3	0	0	0	0	0
Segment: 9	1	0.1	1	0.1	0	0	0	0	0
Segment: 10	7	0.6	5	0.5	1	0.1	0	0	1

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Totals:	309	6.7	92	2.863	150	3.837	0	6	61

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Negative	Comments Submitted
1	Allete - Minnesota Power, Inc.	Jamie Monette		Affirmative	N/A
1	American Transmission Company, LLC	Lauren Price		Negative	Comments Submitted
1	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	John Shaver		Negative	Third-Party Comments
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Joe Tarantino	Negative	Comments Submitted
1	Basin Electric Power Cooperative	David Rudolph		None	N/A
1	BC Hydro and Power Authority	Patricia Robertson		None	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Bonneville Power Administration	Kammy Rogers-Holliday		Negative	Comments Submitted
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		None	N/A
1	Cedar Falls Utilities	Adam Peterson		None	N/A
1	CenterPoint Energy Houston Electric, LLC	John Brockhan		Negative	Comments Submitted
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Hudson Gas & Electric Corp.	Frank Pace		Negative	Comments Submitted
1	City Utilities of Springfield, Missouri	Michael Buyce		Affirmative	N/A
1	CMS Energy - Consumers Energy Company	James Anderson		Negative	Comments Submitted
1	Con Ed - Consolidated Edison Co. of New York	Daniel Grinkevich	Alyson Slanover	Affirmative	N/A
1	Dominion - Dominion Virginia Power	Larry Nash		Negative	Comments Submitted
1	Duke Energy	Doug Hils		Negative	Comments Submitted
1	Edison International - Southern California Edison Company	Steven Mavis		Affirmative	N/A
1	Entergy - Entergy Services, Inc.	Oliver Burke		None	N/A
1	Eversource Energy	Quintin Lee		Affirmative	N/A
1	Exelon	Chris Scanlon		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	Karen Yoder		Affirmative	N/A
1	Great Plains Energy - Kansas City Power and Light Co.	James McBee	Douglas Webb	Affirmative	N/A
1	Great River Energy	Gordon Pietsch		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Negative	Third-Party Comments
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Affirmative	N/A
1	IDACORP - Idaho Power Company	Laura Nelson		Negative	Comments Submitted
1	Imperial Irrigation District	Jesus Sammy Alcaraz		Negative	Comments Submitted
1	International Transmission Company Holdings Corporation	Michael Moltane	Stephanie Burns	Negative	Third-Party Comments
1	Lincoln Electric System	Danny Pudenz		None	N/A
1	Long Island Power Authority	Robert Ganley		None	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	Michael Shaw		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Mike Smith		Affirmative	N/A
1	MEAG Power	David Weekley	Scott Miller	Negative	Third-Party Comments
1	Memphis Light, Gas and Water Division	Allan Long		None	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard		Negative	Third-Party Comments
1	Muscatine Power and Water	Andy Kurriger		Negative	Third-Party Comments
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Negative	Third-Party Comments
1	Nebraska Public Power District	Jamison Cawley		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	New York Power Authority	Salvatore Spagnolo		Negative	Comments Submitted
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		None	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Affirmative	N/A
1	Northeast Missouri Electric Power Cooperative	Kevin White		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Negative	Third-Party Comments
1	Ohio Valley Electric Corporation	Scott Cunningham		Negative	Third-Party Comments
1	Omaha Public Power District	Doug Peterchuck		None	N/A
1	Oncor Electric Delivery	Lee Maurer	Tho Tran	None	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		Negative	Third-Party Comments
1	Peak Reliability	Scott Downey		None	N/A
1	PNM Resources - Public Service Company of New Mexico	Laurie Williams		Negative	Comments Submitted
1	PPL Electric Utilities Corporation	Brenda Truhe		Affirmative	N/A
1	PSEG - Public Service Electric and Gas Co.	Joseph Smith		Affirmative	N/A
1	Public Utility District No. 1 of Chelan County	Jeff Kimbell		None	N/A
1	Public Utility District No. 1 of Snohomish County	Long Duong		Negative	Third-Party Comments
1	Puget Sound Energy, Inc.	Theresa Rakowsky		Negative	Comments Submitted
1	Sacramento Municipal Utility District	Arthur Starkovich	Joe Tarantino	Negative	Comments Submitted
1	Salt River Project	Steven Cobb		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Santee Cooper	Shawn Abrams		Negative	Comments Submitted
1	SCANA - South Carolina Electric and Gas Co.	Tom Hanzlik		Affirmative	N/A
1	Seattle City Light	Pawel Krupa		None	N/A
1	Seminole Electric Cooperative, Inc.	Mark Churilla	Dawn Hamdorf	None	N/A
1	Sempra - San Diego Gas and Electric	Martine Blair	Jeff Johnson	Abstain	N/A
1	Sho-Me Power Electric Cooperative	Peter Dawson		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Katherine Prewitt		Negative	Comments Submitted
1	Southern Indiana Gas and Electric Co.	Steve Rawlinson		None	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell		Negative	Comments Submitted
1	Tennessee Valley Authority	Howell Scott		Negative	Comments Submitted
1	Tri-State G and T Association, Inc.	Tracy Sliman		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Negative	Comments Submitted
1	Westar Energy	Kevin Giles		Negative	Third-Party Comments
1	Western Area Power Administration	sean erickson		Negative	Comments Submitted
1	Xcel Energy, Inc.	Dean Schiro		Negative	Comments Submitted
2	California ISO	Richard Vine		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Elizabeth Axson		Negative	Comments Submitted
2	Independent Electricity System Operator	Leonard Kula		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
2	ISO New England, Inc.	Michael Puscas		None	N/A
2	Midcontinent ISO, Inc.	Terry BIlke		Affirmative	N/A
2	New York Independent System Operator	Gregory Campoli		Negative	Third-Party Comments
2	PJM Interconnection, L.L.C.	Mark Holman		Negative	Third-Party Comments
3	AEP	Aaron Austin		Negative	Comments Submitted
3	AES - Indianapolis Power and Light Co.	Bette White		None	N/A
3	APS - Arizona Public Service Co.	Vivian Vo		Affirmative	N/A
3	Arkansas Electric Cooperative Corporation	Philip Huff		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	W. Dwayne Preston		Affirmative	N/A
3	Basin Electric Power Cooperative	Jeremy Voll		None	N/A
3	BC Hydro and Power Authority	Hootan Jarollahi		None	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Annette Johnston		Negative	Comments Submitted
3	Bonneville Power Administration	Rebecca Berdahl		Negative	Comments Submitted
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City of Farmington	Linda Jacobson-Quinn		None	N/A
3	City of Leesburg	Chris Adkins		Negative	Third-Party Comments
3	City of Vero Beach	Ginny Beigel	Brandon McCormick	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	City Utilities of Springfield, Missouri	Scott Williams		Affirmative	N/A
3	Cleco Corporation	Michelle Corley	Louis Guidry	Negative	Third-Party Comments
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
3	Cowlitz County PUD	Russell Noble		None	N/A
3	Duke Energy	Lee Schuster		Negative	Comments Submitted
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Empire District Electric Co.	Kalem Long		None	N/A
3	Eversource Energy	Mark Kenny		Affirmative	N/A
3	Exelon	John Bee		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Negative	Comments Submitted
3	Great Plains Energy - Kansas City Power and Light Co.	Jessica Tucker	Douglas Webb	Affirmative	N/A
3	Great River Energy	Brian Glover		Negative	Third-Party Comments
3	Hydro One Networks, Inc.	Paul Malozewski		Negative	Third-Party Comments
3	KAMO Electric Cooperative	Ted Hilmes		Affirmative	N/A
3	Lincoln Electric System	Jason Fortik		Negative	Third-Party Comments
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	Manitoba Hydro	Karim Abdel-Hadi		None	N/A
3	MEAG Power	Roger Brand	Scott Miller	Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Modesto Irrigation District	Jack Savage	Nick Braden	Negative	Third-Party Comments
3	Muscatine Power and Water	Seth Shoemaker		Negative	Third-Party Comments
3	National Grid USA	Brian Shanahan		Negative	Third-Party Comments
3	Nebraska Public Power District	Tony Eddleman		Negative	Third-Party Comments
3	New York Power Authority	David Rivera		Negative	Comments Submitted
3	NiSource - Northern Indiana Public Service Co.	Aimee Harris		Affirmative	N/A
3	North Carolina Electric Membership Corporation	doug white	Scott Brame	Negative	Third-Party Comments
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		None	N/A
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
3	Ocala Utility Services	Randy Hahn		Negative	Third-Party Comments
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Negative	Third-Party Comments
3	OTP - Otter Tail Power Company	Wendi Olson		Negative	Third-Party Comments
3	Owensboro Municipal Utilities	Thomas Lyons		Affirmative	N/A
3	Platte River Power Authority	Jeff Landis		Abstain	N/A
3	PNM Resources - Public Service Company of New Mexico	Lynn Goldstein		Negative	Comments Submitted
3	Portland General Electric Co.	Angela Gaines		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	Charles Freibert		Affirmative	N/A
3	PSEG - Public Service Electric and Gas Co.	Jeffrey Mueller		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		None	N/A
3	Puget Sound Energy, Inc.	Tim Womack		None	N/A
3	Rutherford EMC	Tom Haire		Abstain	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Joe Tarantino	Negative	Comments Submitted
3	Salt River Project	Rudy Navarro		Negative	Comments Submitted
3	Santee Cooper	James Poston		Negative	Comments Submitted
3	SCANA - South Carolina Electric and Gas Co.	Clay Young		Affirmative	N/A
3	Seattle City Light	Tuan Tran		Negative	Comments Submitted
3	Seminole Electric Cooperative, Inc.	James Frauen		None	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia	Harold Sherrill	Abstain	N/A
3	Sho-Me Power Electric Cooperative	Jeff Neas		Affirmative	N/A
3	Silicon Valley Power - City of Santa Clara	Val Ridad		None	N/A
3	Snohomish County PUD No. 1	Holly Chaney		None	N/A
3	Southern Company - Alabama Power Company	R. Scott Moore		Negative	Comments Submitted
3	Southern Indiana Gas and Electric Co.	Fred Frederick		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson		Negative	Comments Submitted
3	TECO - Tampa Electric Co.	Ronald Donahey		Negative	Comments Submitted
3	Tennessee Valley Authority	Ian Grant		None	N/A
3	Tri-State G and T Association, Inc.	Janelle Marriott Gill		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Comments Submitted
3	Westar Energy	Bo Jones		Negative	Third-Party Comments
3	Xcel Energy, Inc.	Michael Ibold		Negative	Comments Submitted
4	American Public Power Association	Jack Cashin		None	N/A
4	Arkansas Electric Cooperative Corporation	Alice Wright		Negative	Comments Submitted
4	Austin Energy	Esther Weekes		Affirmative	N/A
4	City of Clewiston	Lynne Mila	Brandon McCormick	Negative	Comments Submitted
4	City Utilities of Springfield, Missouri	John Allen		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Anthony Solic		Affirmative	N/A
4	Georgia System Operations Corporation	Guy Andrews		Negative	Comments Submitted
4	Indiana Municipal Power Agency	Jack Alvey	Scott Berry	Negative	Comments Submitted
4	National Rural Electric Cooperative Association	Barry Lawson		Affirmative	N/A
4	North Carolina Electric Membership Corporation	John Lemire	Scott Brame	Negative	Third-Party Comments
4	Public Utility District No. 1 of Snohomish County	John Martinsen		Negative	Third-Party Comments
4	Sacramento Municipal Utility District	Beth Tincher	Joe Tarantino	Negative	Comments Submitted
4	Seattle City Light	Hao Li		Negative	Comments Submitted
4	Seminole Electric Cooperative, Inc.	Michael Ward		Affirmative	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Shirley Eshbach	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Utility Services, Inc.	Brian Evans-Mongeon		Negative	Comments Submitted
4	WEC Energy Group, Inc.	Anthony Jankowski		Negative	Comments Submitted
5	Acciona Energy North America	George Brown		Negative	Comments Submitted
5	AEP	Thomas Foltz		Negative	Comments Submitted
5	Ameren - Ameren Missouri	Sam Dwyer		None	N/A
5	APS - Arizona Public Service Co.	Linda Henrickson		Affirmative	N/A
5	Arkansas Electric Cooperative Corporation	Moses Harris		Negative	Comments Submitted
5	Associated Electric Cooperative, Inc.	Brad Haralson		Affirmative	N/A
5	Austin Energy	Jeanie Doty		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		None	N/A
5	Basin Electric Power Cooperative	Mike Kraft		None	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		None	N/A
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		Negative	Third-Party Comments
5	Bonneville Power Administration	Francis Halpin		Negative	Comments Submitted
5	BP Wind Energy North America Inc.	Carla Holly		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
5	Cleco Corporation	Stephanie Huffman	Louis Guidry	Negative	Third-Party Comments
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Negative	Comments Submitted
5	Colorado Springs Utilities	Jeff Icke		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Affirmative	N/A
5	Dairyland Power Cooperative	Tommy Drea		Negative	Third-Party Comments
5	Dominion - Dominion Resources, Inc.	Lou Oberski		Negative	Comments Submitted
5	Duke Energy	Dale Goodwine		Negative	Comments Submitted
5	Edison International - Southern California Edison Company	Thomas Rafferty		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		Negative	Comments Submitted
5	Entergy - Entergy Services, Inc.	Jaclyn Massey		Negative	Comments Submitted
5	Exelon	Ruth Miller		Affirmative	N/A
5	FirstEnergy - FirstEnergy Solutions	Robert Loy		Affirmative	N/A
5	Great Plains Energy - Kansas City Power and Light Co.	Harold Wyble	Douglas Webb	Affirmative	N/A
5	Great River Energy	Preston Walsh		Negative	Third-Party Comments
5	Gridforce Energy Management, LLC	David Blackshear		None	N/A
5	Hydro-Qu?bec Production	Normande Bouffard		Abstain	N/A
5	JEA	John Babik		Affirmative	N/A
5	Kissimmee Utility Authority	Mike Blough		Negative	Third-Party Comments
5	Lakeland Electric	Jim Howard		Negative	Third-Party Comments
5	Lincoln Electric System	Kayleigh Wilkerson		Negative	Third-Party Comments
5	Los Angeles Department of Water and Power	Glenn Barry		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Manitoba Hydro	Yuguang Xiao		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	David Gordon		Negative	Comments Submitted
5	MEAG Power	Steven Grego	Scott Miller	Negative	Third-Party Comments
5	Muscatine Power and Water	Neal Nelson		Negative	Third-Party Comments
5	NB Power Corporation	Laura McLeod		Negative	Comments Submitted
5	Nebraska Public Power District	Don Schmit		Negative	Third-Party Comments
5	New York Power Authority	Erick Barrios		Negative	Comments Submitted
5	NextEra Energy	Allen Schriver		None	N/A
5	NiSource - Northern Indiana Public Service Co.	Sarah Gasienica		Affirmative	N/A
5	North Carolina Electric Membership Corporation	Robert Beadle	Scott Brame	Negative	Third-Party Comments
5	Northern California Power Agency	Marty Hostler		Negative	Comments Submitted
5	OGE Energy - Oklahoma Gas and Electric Co.	John Rhea		Negative	Third-Party Comments
5	Omaha Public Power District	Mahmood Safi		Negative	Third-Party Comments
5	Ontario Power Generation Inc.	David Ramkalawan		Affirmative	N/A
5	OTP - Otter Tail Power Company	Cathy Fogale		Negative	Third-Party Comments
5	Portland General Electric Co.	Ryan Olson		None	N/A
5	PPL - Louisville Gas and Electric Co.	Dan Wilson		Affirmative	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Affirmative	N/A
5	Public Utility District No. 1 of Chelan County	Haley Sousa		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Negative	Third-Party Comments
5	Puget Sound Energy, Inc.	Eleanor Ewry		Negative	Comments Submitted
5	Sacramento Municipal Utility District	Susan Oto	Joe Tarantino	Negative	Comments Submitted
5	Salt River Project	Kevin Nielsen		Negative	Comments Submitted
5	Santee Cooper	Tommy Curtis		Negative	Comments Submitted
5	SCANA - South Carolina Electric and Gas Co.	Alyssa Hubbard		Affirmative	N/A
5	Seattle City Light	Mike Haynes		Negative	Comments Submitted
5	Seminole Electric Cooperative, Inc.	Brenda Atkins		None	N/A
5	Sempra - San Diego Gas and Electric	Jerome Gobby	Andrey Komissarov	Abstain	N/A
5	Silicon Valley Power - City of Santa Clara	Sandra Pacheco		None	N/A
5	Southern Company - Southern Company Generation	William D. Shultz		Negative	Comments Submitted
5	SunPower	Bradley Collard		None	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Chris Mattson		Negative	Comments Submitted
5	Talen Generation, LLC	Donald Lock		Negative	Comments Submitted
5	TECO - Tampa Electric Co.	R James Rocha		Negative	Comments Submitted
5	Tennessee Valley Authority	M Lee Thomas		Negative	Comments Submitted
5	U.S. Bureau of Reclamation	Wendy Center		Negative	Comments Submitted
5	WEC Energy Group, Inc.	Linda Horn		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Xcel Energy, Inc.	Gerry Huitt		Negative	Comments Submitted
6	APS - Arizona Public Service Co.	Nicholas Kirby		None	N/A
6	Arkansas Electric Cooperative Corporation	Bruce Walkup		None	N/A
6	Austin Energy	Andrew Gallo		Affirmative	N/A
6	Basin Electric Power Cooperative	Paul Huettl		None	N/A
6	Berkshire Hathaway - PacifiCorp	Sandra Shaffer		Affirmative	N/A
6	Bonneville Power Administration	Andrew Meyers		Negative	Comments Submitted
6	Cleco Corporation	Robert Hirchak	Louis Guidry	Negative	Third-Party Comments
6	Con Ed - Consolidated Edison Co. of New York	Robert Winston		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
6	Duke Energy	Greg Cecil		Negative	Comments Submitted
6	Edison International - Southern California Edison Company	Kenya Streeter		Affirmative	N/A
6	Entergy	Julie Hall		Negative	Comments Submitted
6	Exelon	Becky Webb		Affirmative	N/A
6	FirstEnergy - FirstEnergy Solutions	Ann Ivanc		Affirmative	N/A
6	Florida Municipal Power Pool	Tom Reedy	Brandon McCormick	Negative	Comments Submitted
6	Great Plains Energy - Kansas City Power and Light Co.	Jim Flucke	Douglas Webb	Affirmative	N/A
6	Lincoln Electric System	Eric Ruskamp		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Los Angeles Department of Water and Power	Anton Vu		None	N/A
6	Luminant - Luminant Energy	Brenda Hampton		Affirmative	N/A
6	Manitoba Hydro	Blair Mukanik		Affirmative	N/A
6	Modesto Irrigation District	James McFall	Nick Braden	Negative	Third-Party Comments
6	Muscatine Power and Water	Ryan Streck		Negative	Third-Party Comments
6	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		None	N/A
6	NiSource - Northern Indiana Public Service Co.	Joe O'Brien		Affirmative	N/A
6	Northern California Power Agency	Dennis Sismaet		Negative	Comments Submitted
6	OGE Energy - Oklahoma Gas and Electric Co.	Jerry Nottnagel		Negative	Third-Party Comments
6	Omaha Public Power District	Joel Robles		None	N/A
6	Portland General Electric Co.	Daniel Mason		Affirmative	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
6	Public Utility District No. 1 of Chelan County	Janis Weddle		Negative	Comments Submitted
6	Public Utility District No. 2 of Grant County, Washington	LeRoy Patterson		None	N/A
6	Sacramento Municipal Utility District	Jamie Cutlip	Joe Tarantino	Negative	Comments Submitted
6	Salt River Project	Bobby Olsen		None	N/A
6	Santee Cooper	Michael Brown		Negative	Comments Submitted
6	Seattle City Light	Charles Freeman		Negative	Comments Submitted
6	Seminole Electric Cooperative, Inc.	Trudy Novak		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Snohomish County PUD No. 1	Franklin Lu		None	N/A
6	Southern Company - Southern Company Generation and Energy Marketing	Jennifer Sykes		Negative	Comments Submitted
6	Southern Indiana Gas and Electric Co.	Brad Lisembee		None	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Rick Applegate		Negative	Comments Submitted
6	Talen Energy Marketing, LLC	Jennifer Hohenshilt		None	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		Negative	Comments Submitted
6	Tennessee Valley Authority	Marjorie Parsons		Negative	Comments Submitted
6	WEC Energy Group, Inc.	Scott Hoggatt		Negative	Comments Submitted
6	Westar Energy	Megan Wagner		Negative	Third-Party Comments
6	Xcel Energy, Inc.	Carrie Dixon		Negative	Comments Submitted
7	Exxon Mobil	Jay Barnett		None	N/A
7	Luminant Mining Company LLC	Stewart Rake		Affirmative	N/A
8	David Kiguel	David Kiguel		Affirmative	N/A
8	Massachusetts Attorney General	Frederick Plett		Affirmative	N/A
8	Roger Zaklukiewicz	Roger Zaklukiewicz		Affirmative	N/A
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson		Affirmative	N/A
10	Midwest Reliability Organization	Russel Mountjoy		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	Northeast Power Coordinating Council	Guy V. Zito		Affirmative	N/A
10	ReliabilityFirst	Anthony Jablonski		Affirmative	N/A
10	SERC Reliability Corporation	David Greene		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Negative	Comments Submitted
10	Western Electricity Coordinating Council	Steven Rueckert		None	N/A

Previous 1 Next

Showing 1 to 309 of 309 entries

BALLOT RESULTS

Ballot Name: 2016-02 Modifications to CIP Standards CIP-012-1 Non-binding Poll IN 1 NB
Voting Start Date: 9/1/2017 12:01:00 AM
Voting End Date: 9/11/2017 11:59:59 PM
Ballot Type: NB
Ballot Activity: IN
Ballot Series: 1
Total # Votes: 226
Total Ballot Pool: 290
Quorum: 77.93
Weighted Segment Value: 41.53

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 1	75	1	21	0.447	26	0.553	11	17
Segment: 2	7	0.4	2	0.2	2	0.2	2	1
Segment: 3	70	1	19	0.442	24	0.558	13	14
Segment: 4	14	1	2	0.182	9	0.818	2	1
Segment: 5	69	1	13	0.302	30	0.698	9	17
Segment: 6	42	1	9	0.375	15	0.625	6	12
Segment: 7	2	0.1	1	0.1	0	0	0	1
Segment: 8	3	0.3	3	0.3	0	0	0	0
Segment: 9	1	0.1	1	0.1	0	0	0	0
Segment: 10	7	0.6	5	0.5	1	0.1	0	1
Totals:	290	6.5	76	2.948	107	3.552	43	64

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Negative	Comments Submitted
1	American Transmission Company, LLC	Douglas Johnson		None	N/A
1	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	John Shaver		Negative	Comments Submitted
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Joe Tarantino	Negative	Comments Submitted
1	Basin Electric Power Cooperative	David Rudolph		None	N/A
1	BC Hydro and Power Authority	Patricia Robertson		None	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Negative	Comments Submitted
1	Bonneville Power Administration	Kammy Rogers-Holliday		Negative	Comments Submitted
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		None	N/A
1	Cedar Falls Utilities	Adam Peterson		None	N/A
1	CenterPoint Energy Houston Electric, LLC	John Brockhan		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Hudson Gas & Electric Corp.	Frank Pace		Affirmative	N/A
1	City Utilities of Springfield, Missouri	Michael Buyce		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Daniel Grinkevich	Alyson Slanover	Affirmative	N/A
1	Dominion - Dominion Virginia Power	Larry Nash		Abstain	N/A
1	Duke Energy	Doug Hils		Negative	Comments Submitted
1	Edison International - Southern California Edison Company	Steven Mavis		Affirmative	N/A
1	Entergy - Entergy Services, Inc.	Oliver Burke		None	N/A
1	Eversource Energy	Quintin Lee		Affirmative	N/A
1	Exelon	Chris Scanlon		Abstain	N/A
1	FirstEnergy - FirstEnergy Corporation	Karen Yoder		Affirmative	N/A
1	Great Plains Energy - Kansas City Power and Light Co.	James McBee	Douglas Webb	Affirmative	N/A
1	Great River Energy	Gordon Pietsch		None	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Negative	Comments Submitted
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Affirmative	N/A
1	IDACORP - Idaho Power Company	Laura Nelson		Negative	Comments Submitted
1	Imperial Irrigation District	Jesus Sammy Alcaraz		Abstain	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Stephanie Burns	Negative	Comments Submitted
1	Lincoln Electric System	Danny Pudenz		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Long Island Power Authority	Robert Ganley		None	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	Michael Shaw		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Mike Smith		Affirmative	N/A
1	MEAG Power	David Weekley	Scott Miller	Negative	Comments Submitted
1	Memphis Light, Gas and Water Division	Allan Long		None	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard		Abstain	N/A
1	Muscatine Power and Water	Andy Kurriger		Negative	Comments Submitted
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Negative	Comments Submitted
1	Nebraska Public Power District	Jamison Cawley		Abstain	N/A
1	New York Power Authority	Salvatore Spagnolo		Negative	Comments Submitted
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		None	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Affirmative	N/A
1	Northeast Missouri Electric Power Cooperative	Kevin White		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Negative	Comments Submitted
1	Ohio Valley Electric Corporation	Scott Cunningham		Negative	Comments Submitted
1	Omaha Public Power District	Doug Peterchuck		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	OTP - Otter Tail Power Company	Charles Wicklund		Negative	Comments Submitted
1	Peak Reliability	Scott Downey		None	N/A
1	PNM Resources - Public Service Company of New Mexico	Laurie Williams		Abstain	N/A
1	PPL Electric Utilities Corporation	Brenda Truhe		Abstain	N/A
1	PSEG - Public Service Electric and Gas Co.	Joseph Smith		Abstain	N/A
1	Public Utility District No. 1 of Chelan County	Jeff Kimbell		None	N/A
1	Public Utility District No. 1 of Snohomish County	Long Duong		Negative	Comments Submitted
1	Puget Sound Energy, Inc.	Theresa Rakowsky		Negative	Comments Submitted
1	Sacramento Municipal Utility District	Arthur Starkovich	Joe Tarantino	Negative	Comments Submitted
1	Salt River Project	Steven Cobb		Negative	Comments Submitted
1	Santee Cooper	Shawn Abrams		Abstain	N/A
1	SCANA - South Carolina Electric and Gas Co.	Tom Hanzlik		Affirmative	N/A
1	Seattle City Light	Pawel Krupa		None	N/A
1	Seminole Electric Cooperative, Inc.	Mark Churilla	Dawn Hamdorf	None	N/A
1	Sempra - San Diego Gas and Electric	Martine Blair	Jeff Johnson	Abstain	N/A
1	Sho-Me Power Electric Cooperative	Peter Dawson		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Katherine Prewitt		Negative	Comments Submitted
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Tennessee Valley Authority	Howell Scott		Negative	Comments Submitted
1	Tri-State G and T Association, Inc.	Tracy Sliman		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Negative	Comments Submitted
1	Westar Energy	Kevin Giles		Negative	Comments Submitted
1	Western Area Power Administration	sean erickson		Negative	Comments Submitted
2	California ISO	Richard Vine		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Elizabeth Axson		Affirmative	N/A
2	Independent Electricity System Operator	Leonard Kula		Affirmative	N/A
2	ISO New England, Inc.	Michael Puscas		None	N/A
2	Midcontinent ISO, Inc.	Terry BIlke		Abstain	N/A
2	New York Independent System Operator	Gregory Campoli		Abstain	N/A
2	PJM Interconnection, L.L.C.	Mark Holman		Negative	Comments Submitted
3	AEP	Aaron Austin		Negative	Comments Submitted
3	AES - Indianapolis Power and Light Co.	Bette White		None	N/A
3	APS - Arizona Public Service Co.	Vivian Vo		Affirmative	N/A
3	Arkansas Electric Cooperative Corporation	Philip Huff		Abstain	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	W. Dwayne Preston		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Basin Electric Power Cooperative	Jeremy Voll		None	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Annette Johnston		Negative	Comments Submitted
3	Bonneville Power Administration	Rebecca Berdahl		Negative	Comments Submitted
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City of Farmington	Linda Jacobson-Quinn		None	N/A
3	City of Leesburg	Chris Adkins		Negative	Comments Submitted
3	City of Vero Beach	Ginny Beigel	Brandon McCormick	Negative	Comments Submitted
3	City Utilities of Springfield, Missouri	Scott Williams		Affirmative	N/A
3	Cleco Corporation	Michelle Corley	Louis Guidry	Abstain	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
3	Cowlitz County PUD	Russell Noble		None	N/A
3	Duke Energy	Lee Schuster		Negative	Comments Submitted
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Eversource Energy	Mark Kenny		Affirmative	N/A
3	Exelon	John Bee		Abstain	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Negative	Comments Submitted
3	Great Plains Energy - Kansas City Power and Light Co.	Jessica Tucker	Douglas Webb	Affirmative	N/A
3	Great River Energy	Brian Glover		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Hydro One Networks, Inc.	Paul Malozewski		Negative	Comments Submitted
3	KAMO Electric Cooperative	Ted Hilmes		Affirmative	N/A
3	Lincoln Electric System	Jason Fortik		Abstain	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	Manitoba Hydro	Karim Abdel-Hadi		None	N/A
3	MEAG Power	Roger Brand	Scott Miller	Negative	Comments Submitted
3	Modesto Irrigation District	Jack Savage	Nick Braden	Abstain	N/A
3	Muscatine Power and Water	Seth Shoemaker		Negative	Comments Submitted
3	National Grid USA	Brian Shanahan		Negative	Comments Submitted
3	Nebraska Public Power District	Tony Eddleman		Abstain	N/A
3	New York Power Authority	David Rivera		Negative	Comments Submitted
3	NiSource - Northern Indiana Public Service Co.	Aimee Harris		Affirmative	N/A
3	North Carolina Electric Membership Corporation	doug white	Scott Brame	Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		None	N/A
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
3	Ocala Utility Services	Randy Hahn		Negative	Comments Submitted
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Negative	Comments Submitted
3	OTP - Otter Tail Power Company	Wendi Olson		Negative	Comments Submitted
3	Owensboro Municipal Utilities	Thomas Lyons		Affirmative	N/A
3	Platte River Power Authority	Jeff Landis		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	PNM Resources - Public Service Company of New Mexico	Lynn Goldstein		Abstain	N/A
3	Portland General Electric Co.	Angela Gaines		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	Charles Freibert		None	N/A
3	PSEG - Public Service Electric and Gas Co.	Jeffrey Mueller		Abstain	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		None	N/A
3	Puget Sound Energy, Inc.	Tim Womack		None	N/A
3	Rutherford EMC	Tom Haire		Abstain	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Joe Tarantino	Negative	Comments Submitted
3	Salt River Project	Rudy Navarro		Negative	Comments Submitted
3	Santee Cooper	James Poston		Abstain	N/A
3	SCANA - South Carolina Electric and Gas Co.	Clay Young		Affirmative	N/A
3	Seattle City Light	Tuan Tran		None	N/A
3	Seminole Electric Cooperative, Inc.	James Frauen		None	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia	Harold Sherrill	Abstain	N/A
3	Sho-Me Power Electric Cooperative	Jeff Neas		Affirmative	N/A
3	Silicon Valley Power - City of Santa Clara	Val Ridad		None	N/A
3	Snohomish County PUD No. 1	Holly Chaney		None	N/A
3	Southern Company - Alabama Power Company	R. Scott Moore		Negative	Comments Submitted
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	TECO - Tampa Electric Co.	Ronald Donahey		Negative	Comments Submitted
3	Tennessee Valley Authority	Ian Grant		None	N/A
3	Tri-State G and T Association, Inc.	Janelle Marriott Gill		Affirmative	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Comments Submitted
3	Westar Energy	Bo Jones		Negative	Comments Submitted
3	Xcel Energy, Inc.	Michael Ibold		Abstain	N/A
4	American Public Power Association	Jack Cashin		None	N/A
4	Austin Energy	Esther Weekes		Affirmative	N/A
4	City of Clewiston	Lynne Mila	Brandon McCormick	Negative	Comments Submitted
4	City Utilities of Springfield, Missouri	John Allen		Affirmative	N/A
4	Georgia System Operations Corporation	Guy Andrews		Negative	Comments Submitted
4	Indiana Municipal Power Agency	Jack Alvey	Scott Berry	Negative	Comments Submitted
4	North Carolina Electric Membership Corporation	John Lemire	Scott Brame	Negative	Comments Submitted
4	Public Utility District No. 1 of Snohomish County	John Martinsen		Negative	Comments Submitted
4	Sacramento Municipal Utility District	Beth Tincher	Joe Tarantino	Negative	Comments Submitted
4	Seattle City Light	Hao Li		Negative	Comments Submitted
4	Seminole Electric Cooperative, Inc.	Michael Ward		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Shirley Eshbach	Negative	Comments Submitted
4	Utility Services, Inc.	Brian Evans-Mongeon		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	WEC Energy Group, Inc.	Anthony Jankowski		Negative	Comments Submitted
5	Acciona Energy North America	George Brown		None	N/A
5	AEP	Thomas Foltz		Negative	Comments Submitted
5	Ameren - Ameren Missouri	Sam Dwyer		None	N/A
5	APS - Arizona Public Service Co.	Linda Henrickson		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Brad Haralson		Affirmative	N/A
5	Austin Energy	Jeanie Doty		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		None	N/A
5	Basin Electric Power Cooperative	Mike Kraft		None	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		None	N/A
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		Negative	Comments Submitted
5	Bonneville Power Administration	Francis Halpin		Negative	Comments Submitted
5	BP Wind Energy North America Inc.	Carla Holly		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
5	Cleco Corporation	Stephanie Huffman	Louis Guidry	Abstain	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Negative	Comments Submitted
5	Colorado Springs Utilities	Jeff Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Affirmative	N/A
5	Dairyland Power Cooperative	Tommy Drea		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Dominion - Dominion Resources, Inc.	Lou Oberski		Negative	Comments Submitted
5	Duke Energy	Dale Goodwine		Negative	Comments Submitted
5	Edison International - Southern California Edison Company	Thomas Rafferty		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		Negative	Comments Submitted
5	Entergy - Entergy Services, Inc.	Jaclyn Massey		Negative	Comments Submitted
5	Exelon	Ruth Miller		Abstain	N/A
5	FirstEnergy - FirstEnergy Solutions	Robert Loy		Affirmative	N/A
5	Great Plains Energy - Kansas City Power and Light Co.	Harold Wyble	Douglas Webb	Affirmative	N/A
5	Great River Energy	Preston Walsh		Negative	Comments Submitted
5	Hydro-Qu?bec Production	Normande Bouffard		Abstain	N/A
5	JEA	John Babik		Affirmative	N/A
5	Kissimmee Utility Authority	Mike Blough		Negative	Comments Submitted
5	Lakeland Electric	Jim Howard		Negative	Comments Submitted
5	Lincoln Electric System	Kayleigh Wilkerson		Abstain	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		None	N/A
5	Manitoba Hydro	Yuguang Xiao		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	David Gordon		Abstain	N/A
5	MEAG Power	Steven Grego	Scott Miller	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Muscatine Power and Water	Neal Nelson		Negative	Comments Submitted
5	NB Power Corporation	Laura McLeod		Negative	Comments Submitted
5	Nebraska Public Power District	Don Schmit		Abstain	N/A
5	New York Power Authority	Erick Barrios		Negative	Comments Submitted
5	NextEra Energy	Allen Schriver		None	N/A
5	NiSource - Northern Indiana Public Service Co.	Sarah Gasienica		Affirmative	N/A
5	Northern California Power Agency	Marty Hostler		Negative	Comments Submitted
5	OGE Energy - Oklahoma Gas and Electric Co.	John Rhea		Negative	Comments Submitted
5	Omaha Public Power District	Mahmood Safi		Negative	Comments Submitted
5	Ontario Power Generation Inc.	David Ramkalawan		Affirmative	N/A
5	OTP - Otter Tail Power Company	Cathy Fogale		Negative	Comments Submitted
5	Portland General Electric Co.	Ryan Olson		None	N/A
5	PPL - Louisville Gas and Electric Co.	JULIE HOSTRANDER		None	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A
5	Public Utility District No. 1 of Chelan County	Haley Sousa		Negative	Comments Submitted
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Negative	Comments Submitted
5	Puget Sound Energy, Inc.	Eleanor Ewry		Negative	Comments Submitted
5	Sacramento Municipal Utility District	Susan Oto	Joe Tarantino	Negative	Comments Submitted
5	Salt River Project	Kevin Nielsen		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Santee Cooper	Tommy Curtis		Abstain	N/A
5	SCANA - South Carolina Electric and Gas Co.	Alyssa Hubbard		Affirmative	N/A
5	Seattle City Light	Mike Haynes		Negative	Comments Submitted
5	Seminole Electric Cooperative, Inc.	Brenda Atkins		None	N/A
5	Sempra - San Diego Gas and Electric	Jerome Gobby	Andrey Komissarov	Abstain	N/A
5	Silicon Valley Power - City of Santa Clara	Sandra Pacheco		None	N/A
5	Southern Company - Southern Company Generation	William D. Shultz		Negative	Comments Submitted
5	SunPower	Bradley Collard		None	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Chris Mattson		Negative	Comments Submitted
5	Talen Generation, LLC	Matthew McMillan		None	N/A
5	TECO - Tampa Electric Co.	Frank L Busot		None	N/A
5	Tennessee Valley Authority	M Lee Thomas		None	N/A
5	U.S. Bureau of Reclamation	Wendy Center		Negative	Comments Submitted
5	Westar Energy	Laura Cox		Negative	Comments Submitted
6	APS - Arizona Public Service Co.	Nicholas Kirby		None	N/A
6	Arkansas Electric Cooperative Corporation	Bruce Walkup		None	N/A
6	Austin Energy	Andrew Gallo		Affirmative	N/A
6	Basin Electric Power Cooperative	Paul Huettl		None	N/A
6	Berkshire Hathaway - PacifiCorp	Sandra Shaffer		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Cleco Corporation	Robert Hirchak	Louis Guidry	Abstain	N/A
6	Con Ed - Consolidated Edison Co. of New York	Robert Winston		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
6	Duke Energy	Greg Cecil		Negative	Comments Submitted
6	Edison International - Southern California Edison Company	Kenya Streeter		Affirmative	N/A
6	Entergy	Julie Hall		Negative	Comments Submitted
6	Exelon	Becky Webb		Abstain	N/A
6	FirstEnergy - FirstEnergy Solutions	Ann Ivanc		Affirmative	N/A
6	Florida Municipal Power Pool	Tom Reedy	Brandon McCormick	Negative	Comments Submitted
6	Great Plains Energy - Kansas City Power and Light Co.	Jim Flucke	Douglas Webb	Affirmative	N/A
6	Lincoln Electric System	Eric Ruskamp		Abstain	N/A
6	Los Angeles Department of Water and Power	Anton Vu		None	N/A
6	Luminant - Luminant Energy	Brenda Hampton		Abstain	N/A
6	Manitoba Hydro	Blair Mukanik		Affirmative	N/A
6	Muscatine Power and Water	Ryan Streck		Negative	Comments Submitted
6	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		None	N/A
6	NiSource - Northern Indiana Public Service Co.	Joe O'Brien		Affirmative	N/A
6	Northern California Power Agency	Dennis Sismaet		Negative	Comments Submitted
6	OGE Energy - Oklahoma Gas and Electric Co.	Jerry Nottnagel		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Omaha Public Power District	Joel Robles		None	N/A
6	Portland General Electric Co.	Daniel Mason		Affirmative	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		None	N/A
6	Public Utility District No. 1 of Chelan County	Janis Weddle		Negative	Comments Submitted
6	Public Utility District No. 2 of Grant County, Washington	LeRoy Patterson		None	N/A
6	Sacramento Municipal Utility District	Jamie Cutlip	Joe Tarantino	Negative	Comments Submitted
6	Salt River Project	Bobby Olsen		None	N/A
6	Santee Cooper	Michael Brown		Abstain	N/A
6	Seattle City Light	Charles Freeman		Negative	Comments Submitted
6	Seminole Electric Cooperative, Inc.	Trudy Novak		None	N/A
6	Snohomish County PUD No. 1	Franklin Lu		None	N/A
6	Southern Company - Southern Company Generation and Energy Marketing	Jennifer Sykes		Negative	Comments Submitted
6	Tacoma Public Utilities (Tacoma, WA)	Rick Applegate		Negative	Comments Submitted
6	Talen Energy Marketing, LLC	Jennifer Hohenshilt		None	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		Negative	Comments Submitted
6	Tennessee Valley Authority	Marjorie Parsons		Abstain	N/A
6	WEC Energy Group, Inc.	Scott Hoggatt		Negative	Comments Submitted
6	Westar Energy	Megan Wagner		Negative	Comments Submitted
7	Exxon Mobil	Jay Barnett		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
7	Luminant Mining Company LLC	Stewart Rake		Affirmative	N/A
8	David Kiguel	David Kiguel		Affirmative	N/A
8	Massachusetts Attorney General	Frederick Plett		Affirmative	N/A
8	Roger Zaklukiewicz	Roger Zaklukiewicz		Affirmative	N/A
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson		Affirmative	N/A
10	Midwest Reliability Organization	Russel Mountjoy		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Affirmative	N/A
10	Northeast Power Coordinating Council	Guy V. Zito		Affirmative	N/A
10	ReliabilityFirst	Anthony Jablonski		Affirmative	N/A
10	SERC Reliability Corporation	David Greene		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Negative	Comments Submitted
10	Western Electricity Coordinating Council	Steven Rueckert		None	N/A

Previous 1 Next

Showing 1 to 290 of 290 entries

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2016-02 Modifications to CIP Standards
CIP-012-1

Formal Comment Period Open through September 11, 2017
Ballot Pools Forming through August 25, 2017

Now Available

A 45-day formal comment period for **CIP-012-1 - Cyber Security – Control Center Communication Networks** is open through **8 p.m. Eastern, Monday, September 11, 2017.**

Commenting

Use the electronic form to submit comments. If you experience any difficulties using the electronic form, contact Wendy Muller. An unofficial Word version of the comment form is posted on the project page.

Ballot Pools

Ballot pools are being formed through **8 p.m. Eastern, Friday, August 25, 2017.** Registered Ballot Body members may join the ballot pools here.

If you are having difficulty accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out, contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern).

- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*
- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Next Steps

An initial ballot for the standard and non-binding poll of the associated Violation Risk Factors and Violation Severity Levels will be conducted September 1-11, 2017.

For information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, Katherine Street (via email) or at (404) 446-9702 or Mat Bunch (via email) or at (404) 446-9785.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Comment Report

Project Name:	2016-02 Modifications to CIP Standards | CIP-012-1
Comment Period Start Date:	7/27/2017
Comment Period End Date:	9/11/2017
Associated Ballots:	2016-02 Modifications to CIP Standards CIP-012-1 IN 1 ST

There were 81 sets of responses, including comments from approximately 207 different people from approximately 139 companies representing 10 of the Industry Segments as shown in the table on the following pages.

Questions

1. Requirement R1: The SDT drafted CIP-012-1 Requirement R1 to meet the mandatory requirement for the Responsible Entity to develop one or more documented plan(s) to mitigate the risk of the unauthorized disclosure or modification of data used for Operational Planning Analysis, Real-time Assessment, and Real-time monitoring data while being transmitted between Control Centers. Do you agree with this revision? If not, please provide the basis for your disagreement and an alternate proposal.

2. Requirement R1: The SDT seeks comment on the need to scope sensitive BES data as it applies to Operational Planning Analysis, Real-time Assessment, and Real-time monitoring. Do you agree with scoping CIP-012-1 Requirement R1 in this manner? Please provide comment in support of your response.

3. Implementation Plan: The SDT revised the Implementation Plan such that the standard and NERC Glossary terms are effective the first day of the first calendar quarter that is twelve (12) calendar months after the effective date of the applicable governmental authority's order approving the standard, or as otherwise provided for by the applicable governmental authority. Do you agree with this proposal? If you agree with the proposed implementation time period, please note the actions you will take that require this amount of time to complete. If you think an alternate implementation time period is needed – shorter or longer - please propose an alternate implementation plan and provide a detailed explanation of actions and time needed to meet the implementation deadline.

4. The SDT believes proposed CIP-012-1 provides entities with flexibility to meet the reliability objectives in a cost effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost effective approaches, please provide your recommendation and, if appropriate, technical justification.

5. If you have additional comments on the proposed CIP-012-1 – Cyber Security -- Communication Networks drafted in response to the FERC directive that you have not provided in response to the questions above, please provide them here.

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim	3	RF	FirstEnergy Corporation	Aaron Ghdooshim	FirstEnergy - FirstEnergy Corporation	4	RF
					Aubrey Short	FirstEnergy - FirstEnergy Corporation	1	RF
					Theresa Ciancio	FirstEnergy - FirstEnergy Corporation	3	RF
					Robert Loy	FirstEnergy - FirstEnergy Solutions	5	RF
					Ann Ivanc	FirstEnergy - FirstEnergy Solutions	6	RF
Brandon McCormick	Brandon McCormick		FRCC	FMPA	Tim Beyrle	City of New Smyrna Beach Utilities Commission	4	FRCC
					Jim Howard	Lakeland Electric	5	FRCC
					Lynne Mila	City of Clewiston	4	FRCC
					Javier Cisneros	Fort Pierce Utilities Authority	3	FRCC
					Randy Hahn	Ocala Utility Services	3	FRCC
					Don Cuevas	Beaches Energy Services	1	FRCC
					Jeffrey Partington	Keys Energy Services	4	FRCC
					Tom Reedy	Florida Municipal Power Pool	6	FRCC
					Steven Lancaster	Beaches Energy Services	3	FRCC

					Mike Blough	Kissimmee Utility Authority	5	FRCC
					Chris Adkins	City of Leesburg	3	FRCC
					Ginny Beigel	City of Vero Beach	3	FRCC
Tennessee Valley Authority	Brian Millard	1,3,5,6	SERC	Tennessee Valley Authority	Scott, Howell D.	Tennessee Valley Authority	1	SERC
					Grant, Ian S.	Tennessee Valley Authority	3	SERC
					Thomas, M. Lee	Tennessee Valley Authority	5	SERC
					Parsons, Marjorie S.	Tennessee Valley Authority	6	SERC
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
MRO	Dana Klem	1,2,3,4,5,6	MRO	MRO NSRF	Joseph DePoorter	Madison Gas & Electric	3,4,5,6	MRO
					Larry Heckert	Alliant Energy	4	MRO
					Amy Casucelli	Xcel Energy	1,3,5,6	MRO
					Michael Brytowski	Great River Energy	1,3,5,6	MRO
					Jodi Jensen	Western Area Power Administration	1,6	MRO
					Kayleigh Wilkerson	Lincoln Electric System	1,3,5,6	MRO
					Mahmood Safi	Omaha Public Power District	1,3,5,6	MRO
					Brad Parret	Minnesota Powert	1,5	MRO
					Terry Harbour	MidAmerican Energy Company	1,3	MRO

					Tom Breene	Wisconsin Public Service Corporation	3,5,6	MRO
					Jeremy Voll	Basin Electric Power Cooperative	1	MRO
					Kevin Lyons	Central Iowa Power Cooperative	1	MRO
					Mike Morrow	Midcontinent ISO	2	MRO
SERC Reliability Corporation	David Greene	10	SERC	SERC CIPC	Bill Peterson	SERC RRO	10	SERC
					Mike Hagee	SERC RRO	10	SERC
					SERC CIPC	Various	1,2,5,9	SERC
Con Ed - Consolidated Edison Co. of New York	Dermot Smyth	5	NPCC	Con Edison	Dermot Smyth	Con Edison Company of New York	1,3,5,6	NPCC
					Edward Bedder	Orange & Rockland		NPCC
Seattle City Light	Ginette Lacasse	1,3,4,5,6	WECC	Seattle City Light Ballot Body	Pawel Krupa	Seattle City Light	1	WECC
					Hao Li	Seattle City Light	4	WECC
					Bud (Charles) Freeman	Seattle City Light	6	WECC
					Mike Haynes	Seattle City Light	5	WECC
					Michael Watkins	Seattle City Light	1,4	WECC
					Faz Kasraie	Seattle City Light	5	WECC
					John Clark	Seattle City Light	6	WECC
					Tuan Tran	Seattle City Light	3	WECC
					Laurrie Hammack	Seattle City Light	3	WECC
Santee Cooper	James Poston	3		Santee Cooper	Rene' Free	Santee Cooper	1	SERC
					Rodger Blakely	Santee Cooper	1	SERC
					Chris Jimenez	Santee Cooper	1	SERC

					Troy Lee	Santee Cooper	1	SERC
					Tom Abrams	Santee Cooper	1	SERC
					Jennifer Richards	Santee Cooper	1	SERC
					Stony Martin	Santee Cooper	1	SERC
					Glenn Stephens	Santee Cooper	1	SERC
					Tom Perry	Santee Cooper	1	SERC
Lower Colorado River Authority	Michael Shaw	1		LCRA Compliance	Teresa Cantwell	LCRA	1	Texas RE
					Dixie Wells	LCRA	5	Texas RE
					Michael Shaw	LCRA	6	Texas RE
Southern Company - Southern Company Services, Inc.	Pamela Hunter	1,3,5,6	SERC	Southern Company	Katherine Prewitt	Southern Company Services, Inc.	1	SERC
					R. Scott Moore	Alabama Power Company	3	SERC
					William D. Shultz	Southern Company Generation	5	SERC
					Jennifer G. Sykes	Southern Company Generation and Energy Marketing	6	SERC
Eversource Energy	Quintin Lee	1		Eversource Group	Timothy Reyher	Eversource Energy	5	NPCC
					Mark Kenny	Eversource Energy	3	NPCC
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,8,9,10	NPCC	RSC no Con-Edison and Dominion	Guy V. Zito	Northeast Power Coordinating Council	10	NPCC
					Randy MacDonald	New Brunswick Power	2	NPCC
					Wayne Sipperly	New York Power Authority	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	Orange & Rockland Utilities	3	NPCC
					Michele Tondalo	UI	1	NPCC
					Laura Mcleod	NB Power	1	NPCC
					Michael Schiavone	National Grid	1	NPCC
					Michael Jones	National Grid	3	NPCC
					David Ramkalawan	Ontario Power Generation Inc.	5	NPCC
					Quintin Lee	Eversource Energy	1	NPCC
					Kathleen Goodman	ISO-NE	2	NPCC
					Greg Campoli	NYISO	2	NPCC
					Silvia Mitchell	NextEra Energy - Florida Power and Light Co.	6	NPCC
					Paul Malozewski	Hydro One Networks, Inc.	3	NPCC
					Sylvain Clermont	Hydro Quebec	1	NPCC
					Helen Lainis	IESO	2	NPCC
					Chantal Mazza	Hydro Quebec	2	NPCC
Dominion - Dominion	Sean Bodkin	6		Dominion	Connie Lowe	Dominion - Dominion	3	NA - Not Applicable

Resources, Inc.						Resources, Inc.		
					Lou Oberski	Dominion - Dominion Resources, Inc.	5	NA - Not Applicable
					Larry Nash	Dominion - Dominion Virginia Power	1	NA - Not Applicable
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
					Deborah McEndaffer	Midwest Energy, Inc.	NA - Not Applicable	SPP RE
					Don Schmit	Nebraska Public Power District	5	SPP RE
					Louis Guidry	Cleco Corporation	1,3,5,6	SPP RE
					Robert Hirchak	Cleco Corporation	6	SPP RE
					Marty Paulk	Cleco Corporation	1,3,5,6	SPP RE
					Michelle Corley	Cleco Corporation	3	SPP RE
					Robert Gray	Board of Public Utilities	NA - Not Applicable	SPP RE
					Ron Spicer	EDP Renewables	NA - Not Applicable	SPP RE
					Steven Keller	Southwest Power Pool	2	SPP RE
					Laura Cox	Westar Energy	5	SPP RE

PPL - Louisville Gas and Electric Co.	Shelby Wade	3,5,6	RF,SERC	Louisville Gas and Electric Company and Kentucky Utilities Company	Charles Freibert	PPL - Louisville Gas and Electric Co.	3	SERC
					Dan Wilson	PPL - Louisville Gas and Electric Co.	5	SERC
					Linn Oelker	PPL - Louisville Gas and Electric Co.	6	SERC
PSEG	Sheranee Nedd	1,3,5,6	NPCC,RF	PSEG REs	Tim Kucey	PSEG - PSEG Fossil LLC	5	RF
					Karla Jara	PSEG Energy Resources and Trade LLC	6	RF
					Jeffrey Mueller	PSEG - Public Service Electric and Gas Co	3	RF
					Joseph Smith	PSEG - Public Service Electric and Gas Co	1	RF
ACES Power Marketing	Warren Cross	1,3,4,5	MRO,RF,SERC,SPP RE,Texas RE,WECC	ACES Standards Collaborators	Arizona Electric Power Cooperative, Inc.	AEPC	1	WECC
					Hoosier Energy Rural Electric Cooperative, Inc.	HE	1	RF
					Sunflower Electric Power Corporation	SEPC	1	SPP RE
					Rayburn Country Electric Cooperative	RCEC	3	SPP RE
					Old Dominion Electric Cooperative	ODEC	3,4	SERC
					Brazos Electric Power Cooperative, Inc.	BRAZOS	1,5	Texas RE

					Southern Maryland Electric Cooperative	SMECO	3	RF
					North Carolina Electric Membership Corporation	NCEMC	3,4,5	SERC
					Central Iowa Power Cooperative	CIPCO	1	MRO
					East Kentucky Power Cooperative	EKPC	1,3	SERC
					Buckeye Power, Inc.	BUCK	4	RF

1. Requirement R1: The SDT drafted CIP-012-1 Requirement R1 to meet the mandatory requirement for the Responsible Entity to develop one or more documented plan(s) to mitigate the risk of the unauthorized disclosure or modification of data used for Operational Planning Analysis, Real-time Assessment, and Real-time monitoring data while being transmitted between Control Centers. Do you agree with this revision? If not, please provide the basis for your disagreement and an alternate proposal.

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion

Answer	No
Document Name	

Comment

The term “transmitted between Control Centers” is not clear. Dominion is concerned that the demarcation point between Control Centers is unclear and could cause confusion? A second concern is the potential reliability gap created by the lack of a clarification on whether internal Control Center communications networks are considered to be part of the transmission of data, or if only external communications between entities qualify as transmission data?

Likes 0	
Dislikes 0	

Response

George Brown - Acciona Energy North America - 5

Answer	No
Document Name	

Comment

The term “plan” is misleading in this context. A “plan” is more analogous to the development of a project that has actions to achieve a result by specific date; similar to an implementation plan for a NERC Reliability Standard.

If it was the intention of the SDT to require a Responsible Entity to have a documented set of requirements to protect the sensitive BES data transmitted between the Control Centers then the term “policy” would be more appropriate. A policy is interpreted to be more dynamic and ongoing throughout the lifetime of the requirement. Additionally, as cyber security technology is constantly changing and evolving, a policy would allow for a definite course of action for a Responsible Entity to protect sensitive BES data transmitted between the Control Centers.

Likes 0	
Dislikes 0	

Response

Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino

Answer	No
Document Name	

Comment

It is an overwhelming task to differentiate what is or what isn't confidential communication data over data links between Control Centers. As such, it is recommended that ALL data transmitted between Control Center be protected. The standards should just address all data communication between control centers. Technologies such as encryption are generally implemented by link, not communication type.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	No
Document Name	

Comment

The IESO agrees with the creation of a new standard, rather than expanding CIP-003, CIP-005 and/or CIP-006 requirements to provide new controls over physical communication links. Specifically, the IESO commends the SDT for recognizing that not all utilities own or control their own physical communications links.

The IESO offers the following comments and recommendations.

- R1. For data used for Operational Planning Analysis, Real-time Assessments, and Real-time monitoring, as documented by a Reliability Coordinator, Transmission Operator, or Balancing Authority, the Responsible Entity shall develop one or more documented plan(s) to mitigate the risk of the unauthorized disclosure or modification of the data while it is being transmitted between Control Centers. This excludes oral communications, regardless of transport means.
- The note to R1 concerning the existence of a Control Center or specified data should be a dealt with in Section 4 – Applicability part of the Standard. This would eliminate the need for this to be discussed as part of the RSAW.
- Recommend that it be clarified whether this is a standalone Standard similar to CIP-014 or if it is intended to define the scope of applicable systems to be protected under CIP-003 thru CIP-011.
- In order to evaluate the extent and kind of obligation involved, the definition of between control centers needs to be clearer with regard to the communication link. The Standard should address the proper demarcation points for obligation to show implementation and compliance. To clearly define the obligation of Responsible Entities, the required plan should include identification of the demarcation points. Information is also needed on the explicit agreements required on each end of the physical communication link to arrange and identify such demarcation. Where there is disagreement on how protections are to be applied between two or more Responsible Entities, what is the arbitration process to resolve these disagreements?
- How is the situation handled where a Responsible Entity (e.g., an RC) is receiving information from a third-party provider that is aggregating and submitting data on behalf of one or more Responsible Entities (e.g., a TOP)? What is the identification of the demarcation points? In reading the standard, it does not appear that the connection to the third-party provider is in scope since they are not a Responsible Entity or even registered

with NERC. The same situation may be present for entities that use an outsourced data center provider. The question is also relevant for the data that is provided to regulatory agencies that are not bound by CIP Standards.

Likes 2	Hydro One Networks, Inc., 1, Farahbakhsh Payam; Hydro One Networks, Inc., 3, Malozewski Paul
Dislikes 0	

Response

Dermot Smyth - Con Ed - Consolidated Edison Co. of New York - 5, Group Name Con Edison

Answer	No
Document Name	

Comment

The scope of the term “data” is unclear. Does “data” apply to all data or just machine to machine (e.g. automated) communications? If it is all data would emails/ftp/etc. be in scope?

Likes 0	
Dislikes 0	

Response

Brandon McCormick - Brandon McCormick On Behalf of: Ginny Beigel, City of Vero Beach, 3; Lynne Mila, City of Clewiston, 4; Tom Reedy, Florida Municipal Power Pool, 6; - Brandon McCormick, Group Name FMPA

Answer	No
Document Name	

Comment

FMPA does not agree with the revision of Requirement 1 (R1) because the obligation is not clear. The R1 note - “If the Responsible Entity does not have a Control Center or it does not transmit the type of data specified in Requirement R1 of CIP-012-1 between two Control Centers, the requirements in CIP-012-1 would not apply to that entity.”- should be in the Section 4 Applicability. This would eliminate the need for this to be discussed as part of the RSAW.

In order to evaluate the extent and kind of obligation involved with R1, the phrase “transmitted between two control centers,” needs to be clearer. FMPA believes that there should be more clarity or identification on the demarcation points of the link being protected.

Both TOP-003 and IRO-010 have a requirement that there be a mutually agreeable security protocol. It is not clear why a new standard needs to be developed to address this same issue. The SDT should consider modifying TOP-003 and IRO-010 if these standards do not provide adequate language to meet Order No. 822’s concerns.

Likes 0	
Dislikes 0	

Response

Frank Pace - Central Hudson Gas & Electric Corp. - 1	
Answer	No
Document Name	
Comment	
There is a lack of language within the Requirement that specifies the demarcation point for compliance between applicable Control Centers.	
Likes 0	
Dislikes 0	
Response	
Donald Lock - Talen Generation, LLC - 5	
Answer	No
Document Name	
Comment	
The applicability of the expression, “between Control Centers,” does not appear to be restricted to transmittals between Control Centers owned by a single entity; exchanges between GO and TO/TOP Control Centers would be covered also, for example. This makes sense as regards achieving a high degree of security, but could create confusion regarding who is responsible for inter-entity transmittals. CIP-012-1 should state that GO/GOP obligations for inter-entity exchanges between Control Centers are fulfilled if they follow the data specifications provided by the other party (ref. IRO-010-2 and TOP-003-3).	
Likes 0	
Dislikes 0	
Response	
David Rivera - New York Power Authority - 3	
Answer	No
Document Name	
Comment	
1. The Note to R1 concerning the existence of a Control Center or specified data should be a dealt with in Section 4 – Applicability. This would eliminate the need for this to be discussed as part of the RSAW. 2. In order to evaluate the extent and kind of obligation involved, the definition of between control centers needs to be more clear with regard to the communication link. What are the demarcation points for obligation to show compliance? 3. Request clarification does the 15 minute impact CIP-002 identification of BES Cyber Systems affect the applicability of CIP-012?	
Likes 0	

Dislikes 0	

Response

Philip Huff - Arkansas Electric Cooperative Corporation - 3	
Answer	No
Document Name	

Comment
The Requirement should only permit the option to logically protect the data during transmission or at least remove the explicit options to physically protect the data. We understand the Requirement is consistent with CIP-006 R1.10, but this Requirement addresses communication lines within the same facility, and for which physical protection is possible. Cryptography is the only mechanism available to protect data across geographically dispersed Control Centers. Stating other options is confusing and has a strong potential to guide the industry toward ineffective solutions. However, if the intent is to allow physical protection of communications of Control Centers in the same geographical location, then make it clear in the Technical Guidelines the scenarios and alternative solutions the drafters had in mind.

Likes 0	
Dislikes 0	

Response

Jennifer Hohenshilt - Talen Energy Marketing, LLC - 6	
Answer	No
Document Name	

Comment
The applicability of the expression, “between Control Centers,” does not appear to be restricted to transmittals between Control Centers owned by a single entity; exchanges between GO and TO/TOP Control Centers would be covered also, for example. This makes sense as regards achieving a high degree of security, but could create confusion regarding who is responsible for inter-entity transmittals. CIP-012-1 should state that GO/GOP obligations for inter-entity exchanges between Control Centers are fulfilled if they follow the data specifications provided by the other party (ref. IRO-010-2 and TOP-003-3).

Likes 0	
Dislikes 0	

Response

Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	No
Document Name	

Comment
As mentioned by the SDT, FERC directs *that "…require responsible entities to implement controls to protect, at a minimum, communication links and sensitive bulk electric system data communicated between bulk electric system Control Centers…"*. First, having a plan does not add to the reliability of protecting said data. This is an unwarranted layer of compliance that is not needed. Everything does not need a plan in order to be protected. Recommend that R1 be written in parallel to the FERC directive, which does not require a plan (per the SDTs Consideration of Issues and Directives). If "Plan" is maintained in CIP-012-1 then, the SDT should explain what is meant by having a Plan? Per CIP-003-6 it states, The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter. Is a plan the template document which is used throughout our Standards or is it a set of controls that show that the data is being protected per R1? The NSRF does not understand why a Plan is needed when the data is being protected by physical or electronic means. If a Plan is required, then all the Plan is going to say is that the cabling that transfers data is in a protected conduit (or other means) between Control Centers. Secondly, The NSRF questions why the SDT is not in line with the FERC Order to "…protect …data…" but the proposed R1 states to "…mitigate the risk of unauthorized disclosure or modification of data…"? R1 should be rewritten to state: "The responsible entity shall have controls (or other understandable words) in place to protect against the unauthorized disclosure or modification of BES data used for Operational Planning Analysis, Real-time Assessments, and Real-time monitoring while being transmitted between BES Control Centers. This excludes oral communications". Please note that the word "BES" is needed within R1 regardless of it our proposed rewrite is accepted or not.

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	No
Document Name	

Comment
Texas RE appreciates the Standard Drafting Team's (SDT) efforts to develop a workable approach to mitigate the risk of unauthorized disclosure or modification of certain categories of Control Center communications. However, Texas RE is concerned that the proposed CIP-012-1 R1 does not fully satisfy the directives established by the Federal Energy Regulatory Commission (FERC) in FERC Order No. 822. Texas RE is likewise concerned that the proposed CIP-012-1 may not adequately address third-party entities handling sensitive data between Control Centers in the Texas RE region. First, throughout its discussion concerning new requirements for protecting Control Center communications, FERC emphasized that additional protections were required to protect both the "integrity and availability of sensitive bulk electric system data." FERC Order No. 822, P. 54. FERC made clear that this involved, at a minimum, two discrete actions. First, FERC stressed that entities should implement controls to protect the physical communications links transmitting sensitive data between Control Centers. Second, FERC noted that the sensitive data itself needed to be protected to ensure its accuracy and consistency. In issuing the directive underpinning this rulemaking, FERC stated: "we adopt the NOPR proposal and direct that NERC . . . develop modifications to the CIP Reliability Standards to require responsible entities to implement controls to protect, at a minimum,

communications links and sensitive bulk electric system data communicated between bulk electric system Control Centers . . . FERC Order No. 822, P. 53 (emphasis added).

FERC made it clear that protections should apply to both communication links and sensitive data. However, the proposed draft of CIP-012-1 R1 potentially applies only to physical protections for communications links or to logical protections for data during its transmission. That is, responsible entities could simply elect to plan and implement physical protections for communications links. This would "mitigate" the risk of an unauthorized disclosure or modification of data using one of the delineated methods. As such, the responsible entity would potentially be compliant with the Standard without proposing or implementing any logical protections for sensitive data during its transmission. This appears counter to FERC's intent to protect "both the integrity and availability of sensitive bulk electric system data." FERC Order No. 822, P. 54.

Second, Texas RE is concerned that the proposed CIP-012-1 standard may result in confusion, particularly among Generation Operators with Control Centers subject to the standard regarding the scope of their compliance obligations or, alternatively, may inadvertently result in a significant reliability gap given the structure of the ERCOT market. In ERCOT, generators do not communicate directly with the regional Reliability Coordinator (ERCOT). Instead, generators are required to communicate through designated entities known as Qualified Scheduling Entities (QSEs). In many instances, these QSEs are third-party entities. Within the NERC regulatory construct, Generator Operators have delegated certain NERC compliance functions to these entities, including providing data used for Operational Planning Analysis, Real-time Assessments, and Real-time monitoring. Critically, Generator Operators remain responsible for all compliance obligations associated with QSE activities in the ERCOT region.

In light of this market and regulatory framework, Texas RE interprets the proposed draft of CIP-012-1 to likewise require Generator Operators possessing Control Centers to take steps to mitigate the risk of unauthorized data disclosures at every step along the communication chain between its Control Center and the ERCOT Control Center, including steps to protect this data at third-party intermediary QSEs. Otherwise, the proposed draft of CIP-012-1 would result in a significant reliability gap as QSE communications links and data passing from the QSE to ERCOT could be potentially unsecure. Given this fact, Generator Operators will likely need to take steps to ensure that their third-party QSEs have accorded designated sensitive data appropriate protections, which could in turn require incorporating such requirements into QSE agreements or other steps. Texas RE requests the SDT clarify that communications between QSEs (or equivalent in other Regions) and the RC are subject to CIP-012-1 requirements and that Responsible Entities must take steps to address mitigate the risk of unauthorized data disclosures for these communications as well in order to ensure that Responsible Entities have sufficient notice of these compliance obligations.

Likes 0	
Dislikes 0	

Response

Alice Wright - Arkansas Electric Cooperative Corporation - 4

Answer	No
Document Name	2016-02_CIP-012-1_Comment_Form_07272017-AECC Comments.pdf

Comment

See attachment

Likes 0	
Dislikes 0	

Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	No
Document Name	
Comment	
See APPA Comments.	
Likes 0	
Dislikes 0	
Response	
James Poston - Santee Cooper - 3, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	
Recommend removing “Operational Planning Analysis” from this requirement. Operational Planning Analysis is not Real-time data and would not affect the BES within 15 minutes. The TOP-003-3 Standard currently requires a mutually agreeable security protocol for sharing of data required for Operational Planning Analyses.	
Likes 0	
Dislikes 0	
Response	
Marty Hostler - Northern California Power Agency - 5	
Answer	No
Document Name	
Comment	
NCPA does not feel CIP-012-1 is needed as both TOP-003 R5 and IRO-010 R3 require Registered Entities (REs) to use a mutually agreeable security protocol. The SDT should consider modifying TOP-003 and IRO-010 if these standards do not provide adequate language to meet Order No. 822’s concerns. Also please refer to other APPA, TAPs, and Utility Services comments.	
Likes 0	
Dislikes 0	

Response

Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	

Comment
NCPA does not feel CIP-012-1 is needed as both TOP-003 R5 and IRO-010 R3 require Registered Entities (REs) to use a mutually agreeable security protocol. The SDT should consider modifying TOP-003 and IRO-010 if these standards do not provide adequate language to meet Order No. 822's concerns. Also please refer to other APPA, TAPs, and Utility Services comments.

Likes 0	
Dislikes 0	

Response

David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	No
Document Name	

Comment
The applicability section of the Standard should specify that the requirements only apply to entities with Control Centers. This would allow the elimination of the note to R1 and would simplify the ERO monitoring process.

Likes 0	
Dislikes 0	

Response

Heather Morgan - EDP Renewables North America LLC - 5	
Answer	No
Document Name	

Comment
What does, "Physically protecting the communication links transmitting the data," mean? A Registered Entity is able to physically protect its end point, but is not able to physically protect the communication link for the entire communication link. Please define "logical protection" to provide clarification for entities for implementation and compliance oversight.

What does, “Using an equally effective method to mitigate the risk of unauthorized disclosure or modification of the data” mean?	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	No
Document Name	
Comment	
The Purpose section of CIP-012-1 adds the need to protect the confidentiality of data which is out of Scope of FERC order 822. Although it is recognized that the SDT is not limited to just FERC orders, adding need to protect the confidentiality of data does not add reliability if the data is being protected per CIP-012-1 R1.	
Likes 0	
Dislikes 0	
Response	
Aaron Austin - AEP - 3	
Answer	No
Document Name	
Comment	
AEP suggests that a new requirement(s) be added to establish a hierarchy for REs that requires entities at the top with the most risk to set the communications security protocols. And, modify the existing R1 to require REs to have plans that follow the protocols set by the entities identified in the new requirement(s).	
Likes 0	
Dislikes 0	
Response	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	No
Document Name	

Comment

1. The Note to R1 concerning the existence of a Control Center or specified data should be a dealt with in Section 4 – Applicability. This would eliminate the need for this to be discussed as part of the RSAW.
2. In order to evaluate the extent and kind of obligation involved, the definition of between control centers needs to be more clear with regard to the communication link. What are the demarcation points for obligation to show compliance?
3. Request clarification does the 15 minute impact CIP-002 identification of BES Cyber Systems affect the applicability of CIP-012?
4. Concerns exist with the relationships regarding implementation of CIP-012 with other NERC Standards such as IRO, TOP, CIP-006 R1 Part1.10

Likes 0	
Dislikes 0	

Response

Lona Calderon - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	

Comment

SRP requests the SDT consider differentiating requirements for Control Center communications within an entity from those for Control Center communications between entities. Because data being sent for TOP-003 and IRO-010 traverses over the ICCP network maintained by a carrier, entities cannot provide physical protections for communication of this data from end to end. In this case, protecting the confidentiality and integrity can only be done through encryption. However, since no one utility owns the hardware end to end on the ICCP network, site to site encryption cannot be implemented. The only options available would be application layer encryption or transport layer encryption utilizing IEC 62351-4 Secure ICCP.

For IRO-010 data, the RC in the Western Interconnect requires real-time data to be sent every 10 seconds. Likewise, For TOP-003 data, SRP is required to send and receive real-time data every 10 seconds to and from various other entities on the ICCP network within the Western Interconnect. It is unclear the amount of latency that may be added or amount of computing resources required to encrypt and decrypt this data every 10 seconds. Additionally, the RC would be receiving this data from all applicable utilities in the Western Interconnect. If all entities encrypt and send data every 10 seconds, it is unclear how much latency would be added and computing resources would be required by the RC to decrypt the large amount data. It is also unclear how the added latency would affect the real-time operations of the Bulk Electric System. IRO and TOP data specification changes may be necessary to address delays in data due to latency, or process/procedure changes to mitigate effects on real-time operations. SRP suggests performing a study or survey to determine how much data is being sent and received and what the effects would be from the added latency and the amount of extra computing resources required.

SRP requests clarification on the exclusion of oral communications. Additionally, SRP suggests the exclusion for oral communications be expanded to also exclude electronic mail.

SRP requests clarification for what would be accepted as physical security either in the measures or Technical Rationale and Justification. SRP also requests clarification of what equally effective methods are in the measures or Technical Rationale and Justification.

Likes 0	
Dislikes 0	

Response	
Thomas Breene - WEC Energy Group, Inc. - 3	
Answer	No
Document Name	
Comment	

As mentioned by the SDT, FERC directs *that "…require responsible entities to implement controls to protect, at a minimum, communication links and sensitive bulk electric system data communicated between bulk electric system Control Centers…"*. First, having a plan does not add to the reliability of protecting said data. This is an unwarranted layer of compliance that is not needed. Everything does not need a plan in order to be protected. Recommend that R1 be written in parallel to the FERC directive, which does not require a plan (per the SDTs Consideration of Issues and Directives).

If "Plan" is maintained in CIP-012-1 then, the SDT should explain what is meant by having a Plan? Per CIP-003-6 it states, The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter. Is a plan the template document which is used throughout our Standards or is it a set of controls that show that the data is being protected per R1? We do not understand why a Plan is needed when the data is being protected by physical or electronic means. If a Plan is required, then all the Plan is going to say is that the cabling that transfers data is in a protected conduit (or other means) between Control Centers.

Secondly, we question why the SDT is not in line with the FERC Order to "…protect …data…" but the proposed R1 states to "…mitigate the risk of unauthorized discloser or modification of data…"?

R1 should be rewritten to state: "The responsible entity shall have controls (or other understandable words) in place to protect against the unauthorized disclosure or modification of BES data used for Operational Planning Analysis, Real-time Assessments, and Real-time monitoring while being transmitted between BES Control Centers. This excludes oral communications". Please note that the word "BES" is needed within R1 regardless of it our proposed rewrite is accepted or not.

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 agrees with and support the comments submitted by the MRO Standards Review Forum (NSRF) in regards to this question.

Likes 0	
Dislikes 0	

Response

Russell Noble - Cowlitz County PUD - 3

Answer	No
Document Name	

Comment

Cowlitz PUD supports the comments submitted by APPA.

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Con-Edison and Dominion

Answer	No
Document Name	

Comment

· The Note to R1 concerning the existence of a Control Center or specified data should be a dealt with in Section 4 – Applicability. This would eliminate the need for this to be discussed as part of the RSAW.

· In order to evaluate the extent and kind of obligation involved, the definition of between control centers needs to be clearer with regard to the communication link. What are the demarcation points for obligation to show compliance?

· Request clarification does the 15 minutes impact CIP-002 identification of BES Cyber Systems affect the applicability of CIP-012?

Likes 0	
Dislikes 0	

Response

Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	

Comment

ERCOT ISO signs on to the ITC SWG comments:

The ITC SWG agrees with the creation of a new standard, rather than expanding CIP-003, CIP-005 and/or CIP-006 requirements to provide new controls over physical communication links. Specifically, the ITC SWG commends the SDT for recognizing that not all utilities own or control their own physical communications links.

The ITC SWG offers the following comments and recommendations.

- R1. For data used for Operational Planning Analysis, Real-time Assessments, and Real-time monitoring, as documented by a Reliability Coordinator, Transmission Operator, or Balancing Authority, the Responsible Entity shall develop one or more documented plan(s) to mitigate the risk of the unauthorized disclosure or modification of the data while it is being transmitted between Control Centers. This excludes oral communications, regardless of transport means.
- The note to R1 concerning the existence of a Control Center or specified data should be a dealt with in Section 4 – Applicability part of the Standard. This would eliminate the need for this to be discussed as part of the RSAW.
- Recommend that it be clarified whether this is a standalone Standard similar to CIP-014 or if it is intended to define the scope of applicable systems to be protected under CIP-003 thru CIP-011.
- In order to evaluate the extent and kind of obligation involved, the definition of between control centers needs to be clearer with regard to the communication link. The Standard should address the proper demarcation points for obligation to show implementation and compliance. To clearly define the obligation of Responsible Entities, the required plan should include identification of the demarcation points. Information is also needed on the explicit agreements required on each end of the physical communication link to arrange and identify such demarcation. Where there is disagreement on how protections are to be applied between two or more Responsible Entities, what is the arbitration process to resolve these disagreements?
- How is the situation handled where a Responsible Entity (e.g., an RC) is receiving information from a third-party provider that is aggregating and submitting data on behalf of one or more Responsible Entities (e.g., a TOP)? What is the identification of the demarcation points? In reading the standard, it does not appear that the connection to the third-party provider is in scope since they are not a Responsible Entity or even registered with NERC. The same situation may be present for entities that use an outsourced data center provider. The question is also relevant for the data that is provided to regulatory agencies that are not bound by CIP Standards.

Likes 0	
Dislikes 0	

Response

Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 3	
Answer	No
Document Name	

Comment	
Tacoma Power suuports the commetns of APPA	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1	
Answer	No
Document Name	Project 2016-02_CIP-012-1_NSRF Final.docx
Comment	
WAPA agrees with the comments submitted by the NSRF (attached)	
Likes 0	
Dislikes 0	
Response	
Theresa Rakowsky - Puget Sound Energy, Inc. - 1	
Answer	No
Document Name	
Comment	
See APPA Comments.	
Likes 0	
Dislikes 0	
Response	
Jack Cashin - American Public Power Association - 4	
Answer	No
Document Name	
Comment	

APPA does not agree with the revision of Requirement 1 (R1) because the obligation is not clear. The R1 note - “If the Responsible Entity does not have a Control Center or it does not transmit the type of data specified in Requirement R1 of CIP-012-1 between two Control Centers, the requirements in CIP-012-1 would not apply to that entity.”- should be in the Section 4 Applicability. This would eliminate the need for this to be discussed as part of the RSAW.

Evaluation of the extent and kind of obligation involved with R1, requires a clearer phrase than, “transmitted between two control centers.” Public power believes that there should be more clarity or identification on the demarcation points of the link being protected.

Both TOP-003 and IRO-010 have a requirement that there be a mutually agreeable security protocol. It is not clear why a new standard needs to be developed to address this same issue. The SDT should consider modifying TOP-003 and IRO-010 if these standards do not provide adequate language to meet Order No. 822’s concerns.

Likes 0	
Dislikes 0	

Response

Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	No
Document Name	

Comment

CenterPoint Energy Houston Electric, LLC (“CenterPoint Energy”) recommends adding more clarification on the scope of the term “communication links.” Data used for Operational Planning Analysis (OPA), Real-time Assessments (RTA), and Real-time monitoring (RTM) is collected based on an Entity-issued data specification, per TOP-003-3 and IRO-010-2. This data is collected through a medium referred to as “data exchange capability,” as required by TOP-001-4 (Requirements R19 and R20) as well as IRO-002-5 (Requirements R1 and R2).

OPA data is typically not transmitted via a communication link, and OPA data presents lower risk to operations than real-time telemetry data exchanged via ICCP communication links between Control Centers. The systems used to transmit the OPA data can be located outside Control Centers and are not considered BES Cyber Systems since they do not impact the Bulk Electric System within 15 minutes. Thus, CenterPoint Energy believes OPA data should not be within the scope of Requirement R1.

In addition to removing OPA from Requirement R1, CenterPoint Energy recommends revising Requirement R1 to include the term “inter and intra Control Center communication links.” This revision aligns with the language in Federal Energy Regulatory Commission (“FERC”) Order No. 822. The proposed revised language is below:

“The Responsible Entity shall develop one or more documented plan(s) to mitigate the risk of the unauthorized disclosure or modification of data used for Real-time Assessments and Real-time monitoring while being transmitted between **inter and intra** Control Centers **communication links**. This excludes oral communications.”

Likes 0	
Dislikes 0	

Response

Warren Cross - ACES Power Marketing - 1,3,4,5 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standards Collaborators

Answer	No
Document Name	
Comment	

(1) We agree with the direction of the requirement, however, the wording of the “one of more of” phrase seems to be in conflict with the intention of physical and logical protection. How can you protect the data without physical security, and how can you ensure data integrity without logical protection? The “one or more of” reference should be stricken.

(2) We recommend the addition of wording that clearly excludes Low impact Entities from compliance with this requirement. Would a low impact control room which communicates with a Control Center be out of scope?

(3) We propose moving the compliance applicability note that follows Requirement R1 to the applicability section of the standard, particularly Section 4.2 Exemptions.

Likes 0	
Dislikes 0	
Response	

Michael Puscas - ISO New England, Inc. - 2

Answer	No
Document Name	
Comment	

In order to evaluate the extent and kind of obligation involved, the definition of between control centers needs to be clearer with regard to the communication link. What are the demarcation points for obligation to show compliance? Should there be explicit agreements with each end of the communication link to arrange such demarcation? How should responsible entities deal with third parties involved with trust relationships in communication links (i.e. telecommunications providers managing routers)?

Likes 0	
Dislikes 0	
Response	

David Greyerbiehl - CMS Energy - Consumers Energy Company - 5

Answer	No
Document Name	
Comment	

The requirement as written does not provide clear definition on what type of data needs to be protected, and how exactly the physical/logical protection approach should be accomplished.

Likes 0	
Dislikes 0	

Response

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

BPA appreciates the revisions that the SDT has made based on industry feedback on the SAR.

BPA reiterates its position as documented in our SAR comments that CIP-012-1 is not necessary.

Alternate proposal #1: The objectives can be met by coordinating with existing standards such as CIP-003 and CIP-005.

If CIP-012-1 moves forward, there are areas requiring clarification. FERC Order No. 822 requires implementation of controls to protect, at a minimum, communication links AND sensitive BES data communicated between BES Control Centers. However, the SDT is providing latitude to protect communication links, data or both. If it is an "AND" as stated in Order No. 822, it is not always technically feasible to implement both controls to protect communication links and sensitive BES data communicated between BES Control Centers.

Points of discussion:

Implementation of controls to protect the data:

- Encryption may not be feasible due to availability concerns. (e.g., failure of encryption keys or latency problems with encryption for availability requirements.)

Implementation of controls on communication links:

- The use of the term communication links may be broadly interpreted and difficult to audit.
- It may not be technically feasible to implement physical controls, for example:
    - on fiber optic cable on power lines
    - on a common carrier system where the links are unknown
    - for wireless communications - how does an entity physically protect the air between endpoints?

Additionally, entities and common carriers use a variety of media to carry traffic, and will undoubtedly use traffic shaping to maintain service levels: routing becomes unpredictable; each packet could take a different route from point A to B.

If an entity owns the communication network from end to end, this is still a problem. Modern routing protocols will try to deliver packets over a system with inoperable equipment, severed links, etc. The only remedy is to physically protect the entire communication system in advance of system faults to satisfy CIP-012. If one packet traverses a link due to a system fault that is not protected – it would be a violation.

If FERC agrees with the SDT's proposal of allowing the entity the latitude to protect the data, communication links or both, BPA believes the security objective will not be met. BPA recommends placing controls on the data AND **end points** where technically feasible. However BPA recommends moving R1.1 to a Technical Guidance, considering there are multiple implementation methods for controls on data and end points.

Likes 0	
Dislikes 0	

Response

James Anderson - CMS Energy - Consumers Energy Company - 1

Answer	No
Document Name	

Comment

The requirement as written does not provide clear definition on what type of data need to be protected, and how exactly the physical/logical protection approach should be accomplished by an entity.

Likes 0	
Dislikes 0	

Response

Brian Evans-Mongeon - Utility Services, Inc. - 4

Answer	No
Document Name	

Comment

Utility Services does not agree with the revision of Requirement 1 (R1) because the obligation is not clear. The R1 note - "If the Responsible Entity does not have a Control Center or it does not transmit the type of data specified in Requirement R1 of CIP-012-1 between two Control Centers, the requirements in CIP-012-1 would not apply to that entity."- should be in the Section 4 Applicability. This would eliminate the need for this to be discussed as part of the RSAW.

In order to evaluate the extent and kind of obligation involved with R1, the phrase "transmitted between two control centers", needs to be clearer. Public power believes that there should be more clarity or identification on the demarcation points of the link being protected.

Both TOP-003 and IRO-010 have a requirement that there be a mutually agreeable security protocol. It is not clear why a new standard needs to be developed to address this same issue. The SDT should consider modifying TOP-003 and IRO-010 if these standards do not provide adequate language to meet Order No. 822's concerns.

Likes 0	
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	No
Document Name	

Comment

Southern Company has concerns with the phrase "data used for Operational Planning Analysis, Real-time Assessments, and Real-time monitoring" in CIP-012 R1. We understand this is a direct quote from TOP-003 R1 and IRO-010 R1 and the intent is for this phrase to point to the data specification required by those standards. We understand there is a paragraph to this effect in the Technical Rationale document which is not a binding document. Our concern is that the requirement says "data used for…" and without a stronger bind to the IRO and TOP standards we believe this opens the scope of CIP-012 to yet another data definition exercise rather than a specific requirement to protect an already defined data specification while that data is being transferred between Control Centers.

The draft RSAW for R1 puts this concern in writing. It does not instruct the auditor to use the specifications from TOP-003/IRO-010 Requirement 1 and verify that this previously defined data is protected while being transferred between Control Centers. Instead it requires the auditor to verify

"The documented plan(s) collectively address all data used for Operational Planning Analysis, Real-time Assessments, and Real-time monitoring transmitted between Control Centers"

It then includes glossary definitions for two of those terms. The auditor is instructed to look at two definitions, determine a definition of the undefined "Real-time monitoring", and then verify that all such data is protected. This effort alone dwarfs the true purpose of the standard which is protecting those communications links over which BES Control Centers communicate system status with each other in real time.

We suggest an alternative to resolve this issue. First, we suggest that a data centric approach is problematic for these and other reasons and we strongly suggest a more technical approach that focuses CIP-012 on securing communication sessions and/or links based on their destination. For example, data that is leaving the ESP or LEAP of a Control Center that has a destination address of an ESP or LEAP at another Control Center should be encrypted. That is very distinct and concrete and much simpler to implement and demonstrate and we believe is in line with FERC Order 822, paragraph 60 where the Commission outlines the reliability gap to be addressed.

If this alternative is not acceptable, we suggest that R1 be modified to make the previously defined data specification the noun rather than "data used for…". Additionally, we suggest removing "Operational Planning Analysis" from the first paragraph of R1 as Operational Planning Analysis data does not impact the BES within 15 minutes.

For example: *"The Responsible Entity shall develop one or more documented plan(s) to mitigate the risk of the unauthorized disclosure or modification of data used for Real-time Assessments and Real-time monitoring* ***as specified by the Reliability Coordinator or Transmission Operator*** *while* ***such data*** *is being transmitted between Control Centers. This excludes oral communications."*

We also strongly suggest, based on questions in the draft RSAW, that the SDT consider moving any language relating to applicability to the Applicability section of the standard rather than having a note in the requirement language. With the inclusion of the note in the requirement, we notice

the draft RSAW starts with questions for all the responsible entities that do not have Control Centers to prove the negative, which should instead defer any auditor to the compliance auditing process of CIP-002-5.1.

Likes 0	
Dislikes 0	

Response

Ronald Donahey - TECO - Tampa Electric Co. - 3

Answer	No
Document Name	

Comment

Tampa Electric Company suggests that the SDT provide additional instruction within the standard to address the requirements and implications for BA's that serve as the BA for other entities in the BA's service area. It would be helpful to understand the BA's responsibility to mitigate the risk of unauthorized disclosure or modification of data used for the analysis, assessment and monitoring. In addition, does this standard extend to communications between a Registered Entities and the Reliability Coordinators such as FRCC's RC in relation to communication between Control Centers?

Likes 0	
Dislikes 0	

Response

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group

Answer	No
Document Name	

Comment

The SPP Standards Review Group has reviewed documentation and have developed some concerns in reference to Requirement R1. The CIP Version 5 Transition Advisory Group (V5TAG) identified specific issues with the CIP Version 5 standard language that caused difficulty in implementation of the requirements. This requirement or a supplemental to CIP-005 needs to clarify 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 or a single ESP. This should be address either in this standard, as an Exemption added or requirement added to CIP-005-6.

Here is proposed language for the Exemption:

4.2.3. Exemptions: The following are exempt from Standard CIP -002- 5.1:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety

Commission.

4.2.3.2. *Exemption of Communication Equipment that is owned and operated by a Third Party Communication Carrier or its equivalent is exempted from the CIP standards that is communicating between system end points*

Cyber Assets associated with communication networks and data (striking this information)

communication links between discrete Electronic Security Perimeters. (striking this information)

Or added to CIP-005-6 R1

CIP-005-5 Table R1 – Electronic Security Perimeter

Part

1.6

Applicable

High Impact BES Cyber Systems and their associated:

- *PCA*

Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:

- *PCA*

Requirements

For defined ESPs that use wide-area communications networks (e.g. ESPs that span multiple geographic locations), Cyber Assets associated with communication networks and data communication links used to facilitate the ESP and owned by a third party are exempt from the CIP Reliability Standards provided that the communications traversing across these Cyber Assets are encrypted. The Cyber Assets that encrypt and decrypt the communications are EACMS.

Measures

An example of evidence may include, but is not limited to, network diagrams showing all communication networks, vendor owned equipment, and encryption/decryption Cyber Assets.

There are two major reasons for addressing this issue listed above. 1) This was identified by the V5TAG group and can be easily fixed with one of the two suggestions listed above. Reason 2) is because Registered Entities may expand their ESP's to cover both control centers to handle R1.1 in regards of:

- *Logically protecting the data during transmission; or (Provide example or measures)*
- *Using a measurements to mitigate the risk of unauthorized disclosure or modification of the data.*

Likes 0	
Dislikes 0	

Response	
Wendy Center - U.S. Bureau of Reclamation - 5	
Answer	No
Document Name	
Comment	

Reclamation recommends the SDT use the term “documented processes” consistently throughout the CIP standards. Pursuant to CIP-003-6,

The terms program and plan are sometimes used in place of documented processes where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as plans (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Reclamation disagrees that having a plan adds to the reliability of protecting data used for Operational Planning Analysis, Real-time Assessment, and Real-time monitoring. A plan is an unwarranted layer of compliance that is not needed. Reclamation recommends that R1 be written in parallel with the FERC Order 822, which directed the development of controls to protect communication links and data. Reclamation recommends R1 could be rewritten to state: “The responsible entity shall have documented processes in place to mitigate the risk of the unauthorized disclosure or modification of **BES** data used for Operational Planning Analysis, Real-time Assessments, and Real-time monitoring while being transmitted between BES Control Centers. This excludes oral communications.” Reclamation recommends that the word “BES” be added to R1 regardless of whether the SDT accepts the rest of the above proposed language.

If the requirement for a plan is retained, Reclamation recommends the SDT clarify what is meant by having a plan and how a plan is different from a documented process.

Reclamation recommends using the following definitions of “plan” and “process:”

Plan: Written account of intended future course of action (scheme) aimed at achieving specific goal(s) or objective(s) within a specific timeframe. It explains in detail what needs to be done, when, how, and by whom, and often includes best case, expected case, and worst case scenarios. See also planning.

Process: Sequence of interdependent and linked procedures which, at every stage, consume one or more resources (employee time, energy, machines, money) to convert inputs (data, material, parts, etc.) into outputs. These outputs then serve as inputs for the next stage until a known goal or end result is reached.

Likes 0	
Dislikes 0	
Response	
Scott Berry - Scott Berry On Behalf of: Jack Alvey, Indiana Municipal Power Agency, 1, 4; - Scott Berry	

Answer	No
Document Name	

Comment

We have attached our comments in the last question for the definition of Control Center. We are recommending changes to this definition.

Likes 0	
Dislikes 0	

Response

Lauren Price - American Transmission Company, LLC - 1

Answer	No
Document Name	

Comment

ATC believes the language should be in better alignment with the directives of the FERC order to establish a plan and implement controls to address the risks posed to the BES. ATC also believes the requirement language should be less prescriptive as it relates to data types. ATC believes the Requirement language must allow an appropriate level of flexibility for Registered Entities to identify and document the risks posed to the BES and the corresponding data to assure implemented controls are (and remain) commensurate with risk. The requirement should be focused on the achievement and ongoing sustainability of the security objective in order to permit adaption of their plan(s) and the associated implemented controls such that they are designed to effectively address the current and emerging risks posed to BES Control Center assets and information as the threat landscape changes. Some potential language for consideration is:

“R1. For sensitive Bulk Electric System (BES) data communicated between BES Control Centers, Responsible Entities shall establish and implement one or more documented plans that collectively identifies and addresses:

R1.1. the communication links capable and purposed for the transport of BES data between BES Control Centers

R1.2. the risks posed to the BES from the transport of the BES data between BES Control Centers

R1.2. the BES data subject to the risk

R1.3. the protective measures and security practices designed and implemented to mitigate the identified risks.

R1.4. the process and cycle to review and update the plan(s) to maintain alignment with risks posed

BES data excludes oral communications.”

Likes 0	
Dislikes 0	

Response

James Gower - Entergy - NA - Not Applicable - SERC

Answer	No
Document Name	

Comment

The standard as drafted explicitly excludes oral communications, but does not consider forms of written communication (email, chat, etc) that could communicate the same type of information that an oral communication could. These written instructions are commonly outside of SCADA systems and are on corporate systems, and this standard would require physical or logical controls on those systems for communications that may traverse these systems. The standard should specify the protection of “operational data”, “BCS Data”, or some other term to clarify protection of data outside of instructions, or provide data validation (i.e verify emails by phone) as an acceptable control.

Additionally, Entergy has concerns over expanding the scope of protection from “real-time” as defined in other CIP standards and through existing CIP definitions, to require the protection of Operational Planning Analysis data that is outside of the “real-time” horizon. Requests additional clarity regarding whether the protection is required for data that is used to an input to Operational Planning Analysis, or also includes Operational Planning Analysis data outputs. The Technical Justification and Rationale document seems to imply it is data inputs as it calls out data believed to already be within BES Cyber Systems.

Likes 0	
Dislikes 0	

Response

Guy Andrews - Georgia System Operations Corporation - 4

Answer	No
Document Name	

Comment

- GSOC (Georgia Systems Operations Corporation) requests that the Standards Drafting team provide formal CIP-012 Guidance and Technical Basis (GTB) or Implementation Guidance, either within the Standard or as separate documentation. This is crucial for an entity’s understanding of how to meet the compliance objective of a new Standard.
- GSOC requests clarification regarding:
- he applicability of the Standard to TOs. This Standard should apply only TOs who own or operate Control Centers. An example of modifying the applicability can be found in MOD-025-2.
- the precise nature of Operator-to-Operator communications. “Oral Communications” are excluded. However, EOP-008 (Emergency Operating) Plans often specify using cell/text/email while in mid-failover to the backup site. Would these types of communications also be excluded?
- The Rationale talks about “CIP-012-1 Requirements R1 and R2 protections for applicable data during transmission between two **geographically** separate Control Centers.” However, the requirements themselves don’t seem to make that same distinction. Since the definition of a “Control Center” includes associated data centers, this could lead to the application of this Standard, for example, to a facility that houses 2 control centers side-by-side (one with a data center downstairs). GSOC requests that the Drafting Team provide more information about the Rationale, as it relates to geographical location and proximity of Control Centers, and corresponding language of the Requirements.
- CIP-012 includes protections for data while being transmitted between Control Centers. However, Control Centers are facilities and do not transmit data. Does this include only data transmitted between BES Cyber Systems associated with a Control Center or data transmitted by certified System Operators?

Likes 0	
Dislikes 0	

Response	
Laura McLeod - NB Power Corporation - 5	
Answer	No
Document Name	
Comment	

TOP-003/IRO-010 both require applicable entities have mutual agreement on security protocols. This mutual agreement requirement text of TOP-003/IRO-010 may limit or prevent an entity from following its documented plans of CIP-012-1 R1 should, as an example, either entity change its security protocols.

One approach is to also include the requirement for mutual agreement within CIP-12-1 and/or be more prescriptive in how an entity complies with CIP-012-1 R1 including coordination between entities.

Likes 0	
Dislikes 0	

Response	
Annette Johnston - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	No
Document Name	
Comment	

We do not agree with two separate requirements, one for a plan and one to implement. We recommend following precedent in the other CIP standards, for example, CIP-004-011. The obligation can be accomplished with one requirement, such as follows, with the caveat of concerns expressed in question 1 about what data is covered.

The Responsible Entity shall implement one or more documented processes(s) to mitigate the risk of the unauthorized disclosure or modification of data used for Operational Planning Analysis, Real-time Assessments, and Real-time monitoring while being transmitted between Control Centers, except under CIP Exceptional Circumstances . This excludes oral communications. Risk mitigation shall be accomplished by one or more of the following actions: (follow with the four bullets).

Delete R2.

With one requirement, the note could be simpler by not referencing "R1 of CIP-012-1" and "CIP-012-1." See following.

Note: If the Responsible Entity does not have a Control Center or it does not transmit the type of data specified in this Requirement between two Control Centers, this Requirement would not apply to that entity.

Likes 0	
Dislikes 0	

Response

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1

Answer	No
Document Name	

Comment

See MidAmerican Energy Company comments.

Likes 0	
Dislikes 0	

Response

Laurie Williams - PNM Resources - Public Service Company of New Mexico - 1

Answer	No
Document Name	

Comment

The requirement is too general and would likely not yield consistent compliance among entities and would result in inconsistent auditing of compliance.

Likes 0	
Dislikes 0	

Response

Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 3

Answer	No
Document Name	

Comment

The requirement is too general and would likely not yield consistent compliance among entities and would result in inconsistent auditing of compliance

Likes 0	

Dislikes 0	

Response

Haley Sousa - Public Utility District No. 1 of Chelan County - 5	
Answer	No
Document Name	

Comment
CHPD requests clarification be added to the Technical Rationale for acceptable means of physically protecting communications links and identifying equally effective methods to mitigate risk. CHPD requests that the exclusion for oral communications be extended to electronic mail.

Likes 0	
Dislikes 0	

Response

Janis Weddle - Public Utility District No. 1 of Chelan County - 6	
Answer	No
Document Name	

Comment
CHPD requests clarification be added to the Technical Rationale for acceptable means of physically protecting communications links and identifying equally effective methods to mitigate risk. CHPD requests that the exclusion for oral communications be extended to electronic mail.

Likes 0	
Dislikes 0	

Response

David Greene - SERC Reliability Corporation - 10, Group Name SERC CIPC	
Answer	No
Document Name	3B-2016-02_CIP-012-1_Unofficial_Comment_Form_CIPC.docx

Comment

Likes 0	

Dislikes 0	

Response

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority

Answer	Yes
Document Name	

Comment

TVA agrees, providing the proposed definition of Control Center is adopted.

TVA notes that in many cases some types of operational planning analysis data is housed in systems not classified as BES Cyber Systems and may not reside within an ESP. A documented plan provides a mechanism to identify and document flows of BES sensitive data that do not originate from within an ESP nor pass through an EAP.

Likes 0	
Dislikes 0	

Response

Laura Nelson - IDACORP - Idaho Power Company - 1

Answer	Yes
Document Name	

Comment

IPC does not agree with the need for mandatory requirements. IPC evaluates risks and develops strategies to mitigates those risks, including those associated with communication infrastructure and data transmission. Risks can change, and the implementation of static regulatory obligations that are not flexibly written can make it more difficult to adapt.

Likes 0	
Dislikes 0	

Response

Anthony Jablonski - ReliabilityFirst - 10

Answer	Yes
Document Name	

Comment

Even though ReliabilityFirst votes in the affirmative, ReliabilityFirst provides the following comments for consideration:

1. Requirement R1 –

    i. CIP-012-1 refers to data as outlined in NERC standards TOP-003-3 and IRO-010-2 that are required to be protected. ReliabilityFirst understands these types of data can vary based on entity function and what data is needed. From a compliance monitoring perspective, it may be difficult to verify what the entity is protecting versus what actually should be protected. ReliabilityFirst requests the SDT to consider putting a list of typical data that should be protected per the standard and include it in a guideline document or rationale section.

    ii. The standard, as written, states "Risk mitigation shall be accomplished by one or more of the following actions: Physically protecting the communication links transmitting the data; Logically protecting the data during transmission; or Using an equally effective method to mitigate the risk of unauthorized disclosure or modification of the data." Since this is data in transit (over the "air") ReliabilityFirst inquires on how one provides physical protections? In addition to this, the selection of encryption cyphers, and key lengths are not required. ReliabilityFirst suggests to place some language about encryption in a "technical basis", explaining that there are different cyphers, some better than others, and after weighing the pros and cons of different cyphers and key lengths recommend the use of site-to-site IPV6 encapsulation with a specific cypher and key length.

Likes 0	
Dislikes 0	

Response

Chris Scanlon - Exelon - 1

Answer	Yes
Document Name	

Comment

Exelon agrees with the approach of the latest revision, which provides latitude to protect the communication links, the data, or both, to satisfy the security objective consistent with the capabilities of the Responsible Entity's operational environment.

We do, however, question the placement of the "Note" portion within R1. The Note applies not just to R1, but to CIP-012-1 as a whole. Is there a reason for not including this under Section 4 Applicability, as an exemption?

Likes 0	
Dislikes 0	

Response

Vivian Vo - APS - Arizona Public Service Co. - 3

Answer	Yes
Document Name	2016-02 Modifications to CIP Standards CIP-012-1 - Answer to Question 1.docx

Comment

Please see the attached document for Arizona Public Service Co.'s answer to Question 1.	
Likes 0	
Dislikes 0	
Response	
Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	Yes
Document Name	
Comment	
NRECA agrees with the construct of the standard and its requirements, but not the scope of sensitive BES data as detailed in the response to question 2.	
Likes 0	
Dislikes 0	
Response	
Shelby Wade - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company	
Answer	Yes
Document Name	
Comment	
We support SERC's comments.	
Likes 0	
Dislikes 0	
Response	
David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	

OPG has concerns with potential issues arising from communication links not owned by entity.

Potential issues can also occur when the communication is performed between the CC belonging to different entities; how is the demarcation point determined.

Likes 0	
Dislikes 0	

Response

Mark Riley - Associated Electric Cooperative, Inc. - 1

Answer	Yes
Document Name	

Comment

AECI agrees with the construct of the standard and its requirements, but not the scope of sensitive BES data as detailed in the response to question 2.

Likes 0	
Dislikes 0	

Response

RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Nicholas Lauriat - Network and Security Technologies - 1

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	
Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Shannon Fair - Colorado Springs Utilities - 1,3,5,6, Group Name Colorado Springs Utilities	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 3, Group Name FirstEnergy Corporation	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sheranee Nedd - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	
Likes 1	PSEG - PSEG Fossil LLC, 5, Kucey Tim
Dislikes 0	
Response	
Michael Shaw - Lower Colorado River Authority - 1, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Douglas Webb - Douglas Webb On Behalf of: Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 3, 5, 1, 6; James McBee, Great Plains Energy - Kansas City Power and Light Co., 3, 5, 1, 6; Jessica Tucker, Great Plains Energy - Kansas City Power and Light Co., 3, 5, 1, 6; Jim Flucke, Great Plains Energy - Kansas City Power and Light Co., 3, 5, 1, 6; - Douglas Webb	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	
Document Name	
Comment	
The California ISO supports the comments of the Security Working Group (SWG).	
Likes 0	
Dislikes 0	
Response	

2. Requirement R1: The SDT seeks comment on the need to scope sensitive BES data as it applies to Operational Planning Analysis, Real-time Assessment, and Real-time monitoring. Do you agree with scoping CIP-012-1 Requirement R1 in this manner? Please provide comment in support of your response.

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	
Comment	
See MidAmerican Energy Company comments.	
Likes 0	
Dislikes 0	
Response	

Annette Johnston - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	No
Document Name	
Comment	
The FERC directive refers to "sensitive bulk electric system data" and directs NERC to "identify the scope of sensitive build electric system data." The FERC directive also acknowledges that certain entities are already required to exchange necessary real-time and operational planning data through secured networks using mutually agreeable security protocol. Draft Requirement 1 refers to "data used for Operational Planning Analysis, Real-time Assessments, and Real-time monitoring." We agree with other commenters that these references require revision. Further, we ask the SDT to consider scoping sensitive data explicitly to information exchanged between Control Centers' BES Cyber Systems. This corresponds to SDT's assertation that "this data resides within BES Cyber Systems, and while at rest is protected by CIP-003 through CIP-011." It also corresponds to FERC's recognition of mutually agreeable security protocol networks referenced above.	
Likes 0	
Dislikes 0	
Response	

Laura McLeod - NB Power Corporation - 5	
Answer	No
Document Name	
Comment	

Since Operational Planning Analysis is not real-time data and since planning data/information is generally scrutinized when performing analysis the risk of acting on corrupted data (entry error or unauthorized disclosure/modification) is low.

Likes 0	
Dislikes 0	

Response

Mark Riley - Associated Electric Cooperative, Inc. - 1

Answer	No
Document Name	

Comment

AECI contends that data used for Operational Planning Analysis (OPA) is not sensitive BES data and does not have a 15 minute impact on the reliable operation of the BES. The CIP standards focus on span of control of BES Cyber Systems and their impact to the reliable operation of the BES. Data used for Real-time Assessments and Real-time monitoring can immediately impact the reliable operation of the BES, but data used for OPA has no such impact. AECI requests that the SDT remove OPA from R1 due to not impacting the reliable operation of the BES.

Likes 0	
Dislikes 0	

Response

James Gower - Entergy - NA - Not Applicable - SERC

Answer	No
Document Name	

Comment

Entergy has concerns over expanding the scope of protection from “real-time” as defined in other CIP standards and through existing CIP definitions, to require the protection of Operational Planning Analysis data that is outside of the “real-time” horizon.

Likes 0	
Dislikes 0	

Response

Wendy Center - U.S. Bureau of Reclamation - 5

Answer	No
Document Name	

Comment
Reclamation recommends adding “BES” data to the language as stated above in question 1.

Likes 0	
Dislikes 0	

Response

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	No
Document Name	

Comment
The SPP Standards Review Group has a concern that the scope doesn’t provide the appropriate coverage of the BES data. We would like to propose some new language to address those potential concerns. First of all, a “plan” does not necessarily mean the data is protected. According to the Rationale section FERC is looking for controls to protect these communication links. It should also be clarified that this is “BES” data. The SDT, in the Technical Rationale and Justification document acknowledges TOP-003-3 and IRO-010-2 “provides consistent scoping of identified data” [R1 section: Alignment with IRO and TOP Standards”]. We believe that the data specifications under TOP-003-3 R1 and IRO-010-2 R1 correctly scope the data to be protected; however the current R1 only leaves us with three defined terms for scoping. These 3 defined terms were already used to scope the data specifications under TOP-003-3 R1 and IRO-010-2 R1. CIP-012-1 R1 should reference to TOP-003-1 R1 and IRO-010-2 R1. We realize that it is not the preferred method to reference another Standard; however since CIP-012 is classified as a CIP Standard, and not an Operations and Planning Standard which would be the correct classification, CIP auditors may expand the data to be protected based solely on definitions. In order to properly scope CIP-012, it should reference the TOP-003 and IRO-010 Standards. R1 should be re-written: “The Responsible Entity shall have controls in place to mitigate the risk of the unauthorized disclosure or modification of BES data identified under entity developed data specifications in TOP-003-3 R1 for applicable entities and IRO-010-2 R1 for applicable entities; while such data is being transmitted between BES Control Centers. This excludes oral communications.”

Likes 0	
Dislikes 0	

Response

Ronald Donahey - TECO - Tampa Electric Co. - 3	
Answer	No
Document Name	

Comment
Please provide additional clarification on the protection of load forecasting data as it may not consistently be included as a separate BES Cyber System.

Likes 0	

Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	No
Document Name	

Comment

As per the concern noted in response to question 1, we agree that either further clarification on the scope of the data is needed so it is clear the data in question has already been scoped and is in specifications that are required by IRO-010 and TOP-003, or the SDT should consider setting aside a “data-centric” approach and focus protections on a more technical solution regardless of the data being transmitted between Control Center ESPs and LEAPs.

Likes 0	
Dislikes 0	

Response

Brian Evans-Mongeon - Utility Services, Inc. - 4

Answer	No
Document Name	

Comment

Utility Services does not agree with the scope of the CIP-012-1 R1 as it applies to Operational Planning Analysis, Real-time Assessment, and Real-time monitoring. Since Operational Planning Analysis data would not meet the 15-minute impact criteria used in the identification of BES Cyber Systems, this data would only be required to be protected as it is being transmitted between Control Centers. This inconsistency between the data systems identified by CIP-012-1 and those identified in other CIP standards may cause the unintended expansion of scope of the CIP Standards.

Public power believes applying controls to the Operational Planning Analysis data may reduce the current ability of entities to share this data which may cause a reduction in BES reliability. Not all of this data goes from Control Center to Control Center but may go to (or from) a location outside of a Control Center and therefore would not be in scope of the drafted CIP-012 standard. USI suggests removing the Operational Planning and Analysis data from the scope of this standard.

If the Operational Planning and Analysis data must be retained in the Standard, then USI believes that an exemption for the communication of Operational Planning and Analysis data by email should be put in place. This would be similar to the exemption that exists for voice communication.

Likes 0	
Dislikes 0	

Response	
James Anderson - CMS Energy - Consumers Energy Company - 1	
Answer	No
Document Name	
Comment	
The requirement suggested data are different from those protected in other CIP standards. This may cause confusion in the future by calling it a CIP standard.	
Likes 0	
Dislikes 0	
Response	
David Greyerbiehl - CMS Energy - Consumers Energy Company - 5	
Answer	No
Document Name	
Comment	
The requirement suggested data are different from those protected in other CIP standards. This may cause confusion in the future by calling it a CIP standard.	
Likes 0	
Dislikes 0	
Response	
Warren Cross - ACES Power Marketing - 1,3,4,5 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standards Collaborators	
Answer	No
Document Name	
Comment	
We disagree with the inclusion of Operational Planning Analysis (OPA) based on its NERC definition, as these evaluations are assessed on anticipated and potential conditions for next-day operations and outside the 15-minute impact on the reliable BES operations. The inclusion of OPA is unnecessary and the technical basis does not support it being in scope because it is not impacting the BES in real time.	
Likes 0	
Dislikes 0	

Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	

CenterPoint Energy believes not all data included in OPA, RTA, and RTM is sensitive BES data. CenterPoint Energy recommends the SDT narrow the scope further to only sensitive BES data. Some inputs into OPAs, RTAs, and RTMs (e.g. forecast type data, modeling data such as Facility Ratings, phase angle limitations, etc.) should not be included in the scope of this project. On a situational basis, some telemetry and outage information would also not be considered sensitive BES data.

CenterPoint Energy further recommends that OPA data be completely removed from the scope of CIP-012-1. CenterPoint Energy does not deem this data to be considered sensitive BES data, nor does this data carry the significance of actual Real-time data used for RTAs and RTM.

Likes 0	
Dislikes 0	

Response	
Jack Cashin - American Public Power Association - 4	
Answer	No
Document Name	
Comment	

APPA does not agree with the scope of the CIP-012-1 R1 as it applies to Operational Planning Analysis, Real-time Assessment, and Real-time monitoring. Since Operational Planning Analysis data would not meet the 15-minute impact criteria used in the identification of BES Cyber Systems, this data would only be required to be protected as it is being transmitted between Control Centers. This inconsistency between the data systems identified by CIP-012-1 and those identified in other CIP standards may cause the unintended expansion of scope of the CIP Standards.

Public power believes applying controls to the Operational Planning Analysis data may reduce the current ability of entities to share this data which may cause a reduction in BES reliability. Not all of this data goes from Control Center to Control Center but may go to (or from) a location outside of a Control Center and therefore would not be in scope of the drafted CIP-012 standard. APPA suggests removing the Operational Planning and Analysis data from the scope of this standard.

If the Operational Planning and Analysis data must be retained in the Standard, then APPA believes that an exemption for the communication of Operational Planning and Analysis data by email should be put in place. This would be similar to the exemption that exists for voice communication.

An important consideration with respect to scope and data protection, is the impact encryption may have on the data being considered within the scope of the standard. As SRP communicates in their comments: until the implications are understood about the amount of data being considered for the standard and the impact of encryption on latency and computing resources, the scope may be over-reaching. Therefore, APPA believes that the scoping for the standard does not sufficiently take these factors into account.

Likes 0	

Dislikes 0	
Response	
Theresa Rakowsky - Puget Sound Energy, Inc. - 1	
Answer	No
Document Name	
Comment	
See APPA Comments.	
Likes 0	
Dislikes 0	
Response	
Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 3	
Answer	No
Document Name	
Comment	
Tacoma Power supports the comments of APPA	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	No
Document Name	
Comment	
While we agree with the SDTs approach to align with TOP-003 and IRO-010, we feel that technologies such as encryption or physical protection are generally implemented by link, not communication type.	
Likes 0	
Dislikes 0	
Response	

Russell Noble - Cowlitz County PUD - 3	
Answer	No
Document Name	
Comment	
Cowlitz PUD supports the comments submitted by APPA.	
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 is concerned with the inclusion of BES data used for Operation Planning Analysis that does not have a 15 minute impact on the Bulk Electric System. The inclusion of Operational Planning Assessment data would bring corporate communication links, such as corporate email, into the scope of NERC Standards.

We are also concerned with the language in Requirement R1.1 which states that a method of risk mitigation could be done by "Physically protecting the communication links transmitting data." Xcel Energy believes that the proposed standard does not define what physical controls would be sufficient to mitigate the undefined risk of "unauthorized disclosure of modification of data." Many communication devices owned by Xcel Energy reside in company facilities that have several layers of physical protection. However, once communication links leave our enclosures and ownership purview, physical protection would be difficult at best, largely unknown, and impossible to enforce. The implementation of physical controls only covers a small section of the medium for the data and does not actually protect the data itself. As one of three options; if an organization elects to impement physical controls it would still leave a gap in data integrity and add little benefit with excessive administrative burden.

Xcel Energy respectfully proposes the recommendation for physcial protection to be removed and require logical controls such as encryption, firewalls, information protection release standards and password requirements. Logical controls would more sufficiently protect the data itself end-to-end. We suggest the following edits to R1;

The Responsible Entity shall develop **and implement controls** *[strikethrough:* one or more documented plan(s)] to mitigate the risk of the unauthorized disclosure of or modification to **BES** data used for Operational Planning Analysis, Real-time Assessments, and Real-time monitoring while being transmitted between Control Centers **and which could have an adverse impact on the BES within 15 minutes**. This excludes verbal communications. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. Risk mitigation shall be accomplished by one or more of the following actions:

- [strikethrough: Physically protecting the communication links transmitting the data;]
- Logically protect[strikethrough:ing] the data during transmission; or

- Use[strikethrough:ing] an equally effective method to mitigate the risk of unauthorized disclosure or modification of the data.

Likes 0	
Dislikes 0	

Response

Thomas Breene - WEC Energy Group, Inc. - 3

Answer	No
Document Name	

Comment

The SDT needs to add “BES” data into the language as recommended above in question 1. The “BES data” to be protected should be identified as that “BES data” which can have an impact via high and medium BES Cyber Systems within 15 minutes. In other words, this level of protection should be limited to High and Medium Control Centers and only that data which could put Real-time operations at risk.

Likes 0	
Dislikes 0	

Response

Lona Calderon - Salt River Project - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

SRP agrees this data should be protected. However, after further discussions within SRP and with other entities in the industry, it is clear no one in the industry can state or has an understanding of the implications encryption would have on reliable operation of the BES and the data within this scope. Until a survey or evaluation is performed to understand the amount of data this scope applies to and the impact of encryption on latency and computing resources, the scope may be over-reaching. As such, the manner used for scoping does not adequately take these factors into account.

Likes 0	
Dislikes 0	

Response

Barry Lawson - National Rural Electric Cooperative Association - 4

Answer	No
Document Name	

Comment

NRECA contends that data used for Operational Planning Analysis (OPA) is not sensitive BES data and does not have a 15 minute impact on the reliable operation of the BES. The CIP standards focus on span of control of BES Cyber Systems and their impact to the reliable operation of the BES. Data used for Real-time Assessments and Real-time monitoring can immediately impact the reliable operation of the BES, but data used for OPA has no such impact. We request that the SDT remove OPA from R1 due to not impacting the reliable operation of the BES.

Likes 0	
Dislikes 0	

Response

Aaron Austin - AEP - 3

Answer	No
Document Name	

Comment

AEP suggests that "Operational Planning and Analysis" be removed from R1.

Likes 0	
Dislikes 0	

Response

Quintin Lee - Eversource Energy - 1, Group Name Eversource Group

Answer	No
Document Name	

Comment

The Purpose section of CIP-012-1 adds the need to protect the confidentiality of data which is out of Scope of FERC order 822. Although it is recognized that the SDT is not limited to just FERC orders, adding need to protect the confidentiality of data does not add reliability if the data is being protected per CIP-012-1 R1.

Likes 0	
Dislikes 0	

Response

Vivian Vo - APS - Arizona Public Service Co. - 3

Answer	No

Document Name	

Comment

AZPS respectfully submits that achieving a consensus regarding categorization of data as sensitive across all three interconnections will be difficult – if not impossible – to achieve. The sensitivity of the same data can vary drastically between interconnections and entities within each interconnections. For example, a piece of information that AZPS considers critical and sensitive to its real-time assessments may be viewed as insignificant to another entity. Additionally, certain markets require publication of data that other markets would consider sensitive. Hence, any attempted categorization may conflict with regulatory requirements in Open Access Transmission Tariffs, Market Protocols, state and federal regulations, etc. that obligate entities to disclose and/or that require confidentiality and that are already effective.

Furthermore, such a classification may not matter in practice. The reality is that data flows to Control Centers across a limited number of communication channels. Consider a simplified control center that uses only ICCP for real-time monitoring and assessment, with only half of the data transmitted across that channel being considered "sensitive." It is unlikely that any entity would reasonably determine that it should separate out the sensitive data for protection and leave the non-sensitive data unprotected. It is more likely that they would, instead, protect the entire communication channel. Consequently, AZPS does not support the need or see any benefit to an effort focused on scoping sensitive BES data. Instead, it recommends that responsible entities retain the authority to designate specific data or communication links as "sensitive."

Finally, in the event that the SDT determines a need to scope sensitive BES data, AZPS suggests striking the term "Operational Planning Analysis" from the requirement and limiting the data considered as sensitive to that data which is subject to the NERC Operating Reliability Data (ORD) Agreement. The NERC ORD Agreement is intended to ensure the confidentiality of sensitive data and the definition of Operating Reliability Data and associated obligations included therein are clear, well-established, and well-understood by industry. Importantly, the definition of ORD excludes "Operational Planning Analysis," signaling that such data has not, historically, been considered as "sensitive." Moreover, the Operational Planning Analysis occurs in the next day horizon, providing entities with time to receive and review data prior to use and, where data is suspect, request verification of data or, where data is not timely received, request that such data be re-transmitted. For these reasons, the data utilized in Operational Planning Analyses has extremely limited impact on reliability, which is highly dependent on accurate, appropriate real-time data. Hence, protecting data used in real-time assessment and monitoring as has been required by the NERC ORD Agreement for years is appropriate and the scope of such data has already been evaluated for sensitivity and confidentiality. In summary, if the SDT is compelled to scope sensitive data, to ensure consistency, AZPS recommends that the SDT interpret "sensitive BES data" as encompassing data used in Real-time Assessment and Real-time monitoring only and utilize the NERC ORD Agreement as its primary reference.

Likes 0	
Dislikes 0	

Response

Dennis Sismaet - Northern California Power Agency - 6

Answer	No
Document Name	

Comment

NCPA does not agree with the scope of the CIP-012-1 as it applies to Operational Planning Analysis, Real-time Assessment, and Real-time monitoring. Since Operational Planning Analysis data would not meet the 15-minute impact criteria used in the identification of BES Cyber Systems, this data would only be required to be protected as it is being transmitted between Control Centers. This inconsistency between the data systems identified by CIP-012-1 and those identified in other CIP standards may cause the unintended expansion of scope of the CIP Standards. Also see other APPA and Utility Services/TAPs comments.

Likes 0	

Dislikes 0	
Response	
Marty Hostler - Northern California Power Agency - 5	
Answer	No
Document Name	
Comment	
NCPA does not agree with the scope of the CIP-012-1 as it applies to Operational Planning Analysis, Real-time Assessment, and Real-time monitoring. Since Operational Planning Analysis data would not meet the 15-minute impact criteria used in the identification of BES Cyber Systems, this data would only be required to be protected as it is being transmitted between Control Centers. This inconsistency between the data systems identified by CIP-012-1 and those identified in other CIP standards may cause the unintended expansion of scope of the CIP Standards. Also see other APPA and Utility Services/TAPs comments.	
Likes 0	
Dislikes 0	
Response	
James Poston - Santee Cooper - 3, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	
Recommend removing “Operational Planning Analysis” from this requirement. Operational Planning Analysis is not Real-time data and would not affect the BES within 15 minutes. The TOP-003-3 Standard currently requires a mutually agreeable security protocol for sharing of data required for Operational Planning Analyses.	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	No
Document Name	
Comment	
See APPA Comments.	

Likes 0	
Dislikes 0	
Response	
Alice Wright - Arkansas Electric Cooperative Corporation - 4	
Answer	No
Document Name	
Comment	
See attachment	
Likes 0	
Dislikes 0	
Response	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	No
Document Name	
Comment	
The SDT needs to add “BES” data into the language as recommended above in question 1.	
Likes 0	
Dislikes 0	
Response	
Jennifer Hohenshilt - Talen Energy Marketing, LLC - 6	
Answer	No
Document Name	
Comment	
The question is unclear.	
Likes 0	
Dislikes 0	

Response

Philip Huff - Arkansas Electric Cooperative Corporation - 3	
Answer	No
Document Name	

Comment
Please provide additional guidance on the scope of the information. The Standards from which the scope derives does not provide guidance, and the expansion of scope in CIP-012-1 to all Control Centers necessitates the need for more specific guidance.

Likes 0	
Dislikes 0	

Response

Donald Lock - Talen Generation, LLC - 5	
Answer	No
Document Name	

Comment
The question is unclear.

Likes 0	
Dislikes 0	

Response

Brandon McCormick - Brandon McCormick On Behalf of: Ginny Beigel, City of Vero Beach, 3; Lynne Mila, City of Clewiston, 4; Tom Reedy, Florida Municipal Power Pool, 6; - Brandon McCormick, Group Name FMPA	
Answer	No
Document Name	

Comment
APPA does not agree with the scope of the CIP-012-1 R1 as it applies to Operational Planning Analysis, Real-time Assessment, and Real-time monitoring. Since Operational Planning Analysis data would not meet the 15-minute impact criteria used in the identification of BES Cyber Systems, this data would only be required to be protected as it is being transmitted between Control Centers. This inconsistency between the data systems identified by CIP-012-1 and those identified in other CIP standards may cause the unintended expansion of scope of the CIP Standards. FMPA believes applying controls to the Operational Planning Analysis data may reduce the current ability of entities to share this data which may cause a reduction in BES reliability. Not all of this data goes from Control Center to Control Center but may go to (or from) a location outside of a Control

Center and therefore would not be in scope of the drafted CIP-012 standard. APPA suggests removing the Operational Planning and Analysis data from the scope of this standard.

If the Operational Planning and Analysis data must be retained in the Standard, then APPA believes that an exemption for the communication of Operational Planning and Analysis data by email should be put in place. This would be similar to the exemption that exists for voice communication.

Likes 0	
Dislikes 0	

Response

Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino

Answer	No
Document Name	

Comment

We are concerned because unauthorized alteration of Operational Planning Analysis data does not pose a threat to the BES. This more appropriately addressed by TOP 010-1 reliability standard regarding the quality of the data. We note that Operational Planning Data is not real time data, as such we ask the STD to treat communicating Operational Planning Data Email exempt similar to the oral communication.

Likes 0	
Dislikes 0	

Response

George Brown - Acciona Energy North America - 5

Answer	No
Document Name	

Comment

The requirement as written does not meet the criteria as outlined in the document titled “Ten Benchmarks of an Excellent Reliability Standard”, benchmark 8. Clear Language. As the SDT stated in the rationale, the data in scope is the data as specified in TOP-003-3 and IRO-010-2. If this is in fact the case then the SDT should draw a clear and unambiguous line to these standards within the requirement. The addition of such language will also prevent unintentional scope reach.

Suggested language should be something to the following effect:

R1.2 The Responsible Entity, as applicable to its registered function, shall consider the data used for Operational Planning Analysis, Real-time Assessments, and Real-time monitoring to be the data as specified in:

- NERC Reliability Standard IRO-010-2, Requirement R1 and,
- NERC Reliability Standard TOP-003-3 — Operational Reliability Data, Requirement R1 and Requirement R2.

Likes 0	
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion

Answer	No
Document Name	

Comment

Dominion asserts that data used for Operational Planning Analysis is often an ad-hoc report by exception (e.g., this line will be out or this unit will be de-rated) and because this data is often collected by a stand-alone system it can often be entered by several people within an organization and from several locations. Dominion is unclear on whether the entity expected to track which data is specifically entered from within a Control Center as opposed to from an office external to the Control Center. Many stand-alone systems are web-based and use https for all transactions. It is unclear what would qulaify as adequate evidence and that tracking locations and persons entering the information is not necessary.

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

Duke Energy has concerns about the decision to add Operational Planning Analysis information to the scope of the data protected by this standard. Currently, the scope of the CIP standards primarily focuses on real-time data, and bringing in Operational Planning Analysis pushes the scope of CIP standards to include Day Ahead. Also, in some instances, Operational Planning Analyses can be performed by a 3rd party or require data transmitted between entities via 3rd party tools. How would these affect be impacted by the applicability of the standard? Extending the CIP scope to apply to Day Ahead data is a departure, and could broaden the view of what tools (possibly including web-based tools?) could fall under CIP scope.

Likes 0	
Dislikes 0	

Response

RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC	
Answer	No
Document Name	
Comment	
If there is the need to scope sensitive BES data as it applies to Operational Planning Analysis, Real-time Assessment, and Real-time monitoring, it should all be scoped as data of the High Impact BES Cyber Systems.	
Likes 0	
Dislikes 0	
Response	
Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 3	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lauren Price - American Transmission Company, LLC - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Greene - SERC Reliability Corporation - 10, Group Name SERC CIPC	
Answer	No

Document Name	3B-2016-02_CIP-012-1_Unofficial_Comment_Form_CIPC.docx
Comment	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Guy Andrews - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
We request clarification on the inclusion of data used for Operational Planning Analysis. This data does not have a 15 minute impact on the Bulk Electric System. This data is also typically exchanged between operations engineering staff who would not be considered to be a Control Center.	
Likes 0	
Dislikes 0	
Response	
Michael Shaw - Lower Colorado River Authority - 1, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	

Please provide guidance on whether or not email is in scope as a communication medium.	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
However, BPA questions the inclusion of Operational Planning Analysis.	
Likes 0	
Dislikes 0	
Response	
Sheranee Nedd - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	
RC, TOP and BA functional entities develop and disseminate specifications for the BES data they need to conduct Operational Planning Analysis, Real-time Assessment, and Real-time monitoring, in NERC '693' reliability standards TOP-003 and IRO-010. Relevant peer RCs/TOPs/BAs and others (GOs; GOPs; TOs; LSEs; DPs) are required by these standards to meet these data specifications. The scope of data subject to R1 is (or should be) thereby understood to be the data that entities both (i) specify in observance of these standards and (ii) transmit between the entity's and others' Control Centers.	
Likes 1	PSEG - PSEG Fossil LLC, 5, Kucey Tim
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1	
Answer	Yes
Document Name	
Comment	

Exelon agrees that aligning with TOP-003-3 and IRO-010-2 is helpful for scoping CIP-012-1, and promotes consistent application of the NERC Standards.	
Likes 0	
Dislikes 0	
Response	
David Rivera - New York Power Authority - 3	
Answer	Yes
Document Name	
Comment	
No Comment	
Likes 0	
Dislikes 0	
Response	
Dermot Smyth - Con Ed - Consolidated Edison Co. of New York - 5, Group Name Con Edison	
Answer	Yes
Document Name	
Comment	
Same comment as question #1 above.	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
In the event mandatory standards are imposed, the scope should be limited to data that have well-defined terms.	

Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
TVA agrees that the entity needs to know what information is classified as BES sensitive data as it relates to operational planning analysis, real-time assessment, and real-time monitoring. In many cases some types of operational planning analysis data is housed in systems not classified as BES Cyber Systems and may not reside within an ESP.	
Likes 0	
Dislikes 0	
Response	
Janis Weddle - Public Utility District No. 1 of Chelan County - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb On Behalf of: Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 3, 5, 1, 6; James McBee, Great Plains Energy - Kansas City Power and Light Co., 3, 5, 1, 6; Jessica Tucker, Great Plains Energy - Kansas City Power and Light Co., 3, 5, 1, 6; Jim Flucke, Great Plains Energy - Kansas City Power and Light Co., 3, 5, 1, 6; - Douglas Webb	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Haley Sousa - Public Utility District No. 1 of Chelan County - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laurie Williams - PNM Resources - Public Service Company of New Mexico - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Puscas - ISO New England, Inc. - 2	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Con-Edison and Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Heather Morgan - EDP Renewables North America LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 3, Group Name FirstEnergy Corporation	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Shannon Fair - Colorado Springs Utilities - 1,3,5,6, Group Name Colorado Springs Utilities	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Frank Pace - Central Hudson Gas & Electric Corp. - 1	
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	
Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Nicholas Lauriat - Network and Security Technologies - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE does not have comments on this question.	
Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	
Document Name	
Comment	
The California ISO supports the comments of the Security Working Group (SWG).	
Likes 0	
Dislikes 0	
Response	

3. Implementation Plan: The SDT revised the Implementation Plan such that the standard and NERC Glossary terms are effective the first day of the first calendar quarter that is twelve (12) calendar months after the effective date of the applicable governmental authority's order approving the standard, or as otherwise provided for by the applicable governmental authority. Do you agree with this proposal? If you agree with the proposed implementation time period, please note the actions you will take that require this amount of time to complete. If you think an alternate implementation time period is needed – shorter or longer - please propose an alternate implementation plan and provide a detailed explanation of actions and time needed to meet the implementation deadline.

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

Answer	No
Document Name	

Comment

Duke Energy disagrees with the proposed 12 month Implementation Plan. Certain aspects of achieving compliance with this standard (for example, implementing end to end encryption) would, in some instances, take a significant amount of time to put in place to due to the significance of the impact of these changes on critical systems. Further, applying these protections between Control Centers owned by more than one Responsible Entity will involve significant coordination, and additional time would be necessary to develop a shared understanding of existing technical limitations, develop agreements, and implement those new approaches for compliance. Duke Energy suggests that a phased implementation plan would be appropriate given the action necessary. We encourage the drafting team to consider an Implementation Plan of 12 months for R1. This would give time for the Responsible Entity to assess the Control Centers that are in its scope, decide on a method of protection, and involve any additional parties that may be necessary. We suggest a minimum of 24 months for the implementation date for R2 (implementing the plan developed in R1).

Likes 0	
Dislikes 0	

Response

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority

Answer	No
Document Name	

Comment

TVA does not agree that twelve months is sufficient time to coordinate with other entities to agree on and implement protection mechanisms. Implementation may require coordination of plans across a large and/or diverse group of entities employing a variety of protective measures. TVA suggests 18-24 months would be a more realistic implementation period.

Likes 0	
Dislikes 0	

Response

Laura Nelson - IDACORP - Idaho Power Company - 1

Answer	No

Document Name	
Comment	
Changes take time to evaluate and implement. The communication lines will have to be inventoried and evaluated. The data traveling across these lines will have to be inventoried and evaluated to ensure entities can evidence that they are protecting the itemized list of data included in the wording of R1 (Operational Planning Analysis, Real-time Assessment, and Real-time monitoring). Other activities that would need to occur for successful implementation would include preparation and delivery of guidance by regulatory bodies, communication and coordination with partner entities, configuration, and testing. At minimum, an 18-month implementation plan would be appropriate.	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	
Comment	
Dominion asserts that budgets, resources, and other events between separate entities may require periods greater than 12 months. Dominion recommends that the implementation period be revised to 24 months.In addition, the time required to develop (R1), and then successfully implement (R2) would take longer than 12 months from the start date. 24 months should allow sufficient time to accomplish implementation of both requirements.	
Likes 0	
Dislikes 0	
Response	
George Brown - Acciona Energy North America - 5	
Answer	No
Document Name	
Comment	
This standard will require a collaborative effort between Control Centers of the various applicable Functional Entities to achieve the securities as required. As such, it may not feasible for some entities to implement these securities within 12 months. For example, a Reliability Coordinator (RC) Control Center will have contact with the Control Centers of several Balancing Authorities (BA), Generator Operators (GOP), Transmission Operators (TOP), Transmission Owners (TO) and other RCs. If a particular RC is unable to support the implementation of the securities as required in NERC CIP-012-1 then there will be a cascading and unnecessary non-compliance effect among the other Functional Entities that have Control Centers that transmit and receive this sensitive BES data with this particular RC's Control Center. A phase-in approach may be more appropriate for NERC CIP-012-1, based on schedules created using the Function Entity reliability hierarchy structure.	
Likes 0	

Dislikes 0	

Response

Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino	
Answer	No
Document Name	

Comment
For complex entities the identification and agreement on communication protocols and architecture may require extensive testing and learning. We recommend at least 18 months due to the quantity of details and logistics.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	

Comment
The IESO also encourages the drafting team to make the requirement forward-looking in regards to contracts currently in place. Provisions should be set for legacy contracts including grandfathering of existing agreements and equipment. Implementation of controls involving telecommunications providers will require coordination and scheduling to align to the providers' resource availability and reduce adverse impact on reliability. This should not require renewal and renegotiation of existing contracts until they reach the end of the existing contract period. It should be noted that it is difficult to determine suitability of the implementation timeline when there are open questions about the viability of available solutions for adequate protections. More time is necessary to allow for coordination with a large number of parties. This will require budgeting, planning, and scheduling with external resources for implementation. It will also require significant testing and validation by parties on both ends of a connection. The IESO recommends a phased implementation with defined milestones similar to CIP-014. Consider the following:

- For creation of the plan, 12 months should be allowed to (1) conduct an impact assessments, (2) identify the approach to be included in the plan, (3) implementation milestones, and (4) implementation schedule. This could identify the communication links that have protections currently in place. The plan could also include identifying all links and protections requiring changes to address service contracts and related relationships to adjust for new protections. The plan could then be approved by an appropriate entity.

- For implementation of the plan, additional time should be allowed for budgeting, planning, and scheduling with external resources. This includes planning with other Responsible Entities as well as telecommunications providers.

Likes 2	Hydro One Networks, Inc., 1, Farahbakhsh Payam; Hydro One Networks, Inc., 3, Malozewski Paul
Dislikes 0	

Response

Brandon McCormick - Brandon McCormick On Behalf of: Ginny Beigel, City of Vero Beach, 3; Lynne Mila, City of Clewiston, 4; Tom Reedy, Florida Municipal Power Pool, 6; - Brandon McCormick, Group Name FMPA

Answer	No
Document Name	

Comment

FMPA does not agree with the implementation proposal timeline. The time to implement R1 (develop a plan) should be 12 months from the time of the order.

Due to technical complexity, agreements (outsourced and between registered entities), procurement, contracts and coordination between registered entities (and provisioning of private networks), FMPA requests that the SDT consider the following options for R2 implementation:

- additional 24 months allowed to undertake implementation,

- using a phased implementation over a five or longer year period, or

- in recognition that there is the potential for several existing contracts will have to be replaced (and associated equipment) that affected contracts be grandfathered until new and or, replacements can be put in place.

Likes 0	
Dislikes 0	

Response

Frank Pace - Central Hudson Gas & Electric Corp. - 1

Answer	No
Document Name	

Comment

It would appear that the proposed implementation period is too short; however, it is difficult to determine if a demarcation point for compliance is not specified within the language of the Requirement.

Likes 0	
Dislikes 0	

Response

Donald Lock - Talen Generation, LLC - 5

Answer	No
Document Name	

Comment

The 12-month period provided in the implementation plan should be at least doubled. Developing a clear understanding of what is required could take some time, and to then scope the project, obtain bids and budget approval, receive materials and implement in whatever portion of the year remains may prove impractical.

Likes 0	
Dislikes 0	

Response

David Rivera - New York Power Authority - 3

Answer	No
Document Name	

Comment

1. The time to implement R1 (develop plan) could be 12 months from time of order. For implementation of R2 there should be an additional 24 months allowed to undertake implementation. This would include identifying all links and protections, with changes needed to address communications service contracts and related relationships to adjust for new protections. This would also involve inventory of data to comply with identification of all data transmitted between control centers.
2. Due to technical complexity, agreements (outsourced and between Entities), procurement, contracts and coordination between Entities (and provisioning of private networks), request that the SDT also consider the following option for R2 implementation:
    i. a phased implementation over a five or longer year period, or
    ii. to avoid impacting reliability, existing contracts, equipment, etc be grandfathered until new / replacements are in place.

Likes 0	
Dislikes 0	

Response

Jennifer Hohenshilt - Talen Energy Marketing, LLC - 6

Answer	No
Document Name	
Comment	
The 12-month period provided in the implementation plan should be at least doubled. Developing a clear understanding of what is required could take some time, and to then scope the project, obtain bids and budget approval, receive materials and implement in whatever portion of the year remains may prove impractical.	
Likes 0	
Dislikes 0	
Response	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	No
Document Name	
Comment	
The 12 month time period may only work for Entities who are vertically intergraded. The flow of applicable BES data within CIP-012-1 can be viewed as a “spider web” of data transfer for large RC foot-prints. With this being said, there may be non-compliance issues when one side of the data transference is protected and the other side is not. The SDT should propose a phased in approach to protecting data. A five (5) year implementation plan will allow entities to fund these projects. This is especially important to small entities. Per the NERC Guidance concerning “Phase Implementation Plans with Completion Percentages (http://www.nerc.com/pa/comp/guidance/CMEPPracticeGuidesDL/CMEP_Practice_Guide_Phased_Implementation_Completion_Percentages.pdf) please state that the CIP-012-1 does not fall under this guidance.	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	No
Document Name	
Comment	
See APPA Comments.	
Likes 0	
Dislikes 0	

Response

James Poston - Santee Cooper - 3, Group Name Santee Cooper

Answer	No
Document Name	

Comment
Recommend a 2 year Implementation Plan Period. For some entities, it may take a significant amount of time to agree on communication protocols and architecture with neighboring systems. Time is also needed to troubleshoot and test each connection point.

Likes 0	
Dislikes 0	

Response

Marty Hostler - Northern California Power Agency - 5

Answer	No
Document Name	

Comment
NCPA does not agree with the implementation proposal timeline. Due to technical complexity, agreements (outsourced and between REs), procurement, contracts and coordination between REs (and provisioning of private networks), NCPA requests that the SDT consider the following options for R2 implementation: • additional 24 months allowed to undertake implementation, • using a phased implementation over a five or longer year period, or • in recognition that there is the potential for several existing contracts will have to be replaced (and associated equipment) that affected contracts be grandfathered until new and or, replacements can be put in place.

Likes 0	
Dislikes 0	

Response

Dennis Sismaet - Northern California Power Agency - 6

Answer	No
Document Name	

Comment
NCPA does not agree with the implementation proposal timeline. Due to technical complexity, agreements (outsourced and between REs), procurement, contracts and coordination between REs (and provisioning of private networks), NCPA requests that the SDT consider the following options for R2 implementation: • additional 24 months allowed to undertake implementation, • using a phased implementation over a five or longer year period, or • in recognition that there is the potential for several existing contracts will have to be replaced (and associated equipment) that affected contracts be grandfathered until new and or, replacements can be put in place.

Likes 0	
Dislikes 0	

Response

Vivian Vo - APS - Arizona Public Service Co. - 3	
Answer	No
Document Name	

Comment
The proposed implementation plan does not consider complexities associated with implementing technical solutions reliant on inter-entity coordination and agreement. The proposed implementation plan does not recognize the prerequisite of mutual agreement between entities regarding a compatible technical solution or the time necessary to complete such prerequisite. Moreover, it does not appear to contemplate a potential need for dispute resolution when a transmitting entity and receiving entity cannot agree on a solution. Finally, any implementation, testing, etc. can only occur once the mutually agreed-upon solution has been identified, budgeted, and procured. For these reasons, AZPS proposes extending the implementation plan to at least twenty-four (24) calendar months. Two years would likely allot adequate time to identify, agree upon, and procure appropriate technical solutions in coordination with other entities.

Likes 0	
Dislikes 0	

Response

David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	No
Document Name	

Comment

The Implementation Plan should be modified to allow 24 months for the implementation phase (R2) due to the potential impact resulting from the necessity of redesigning communications architectures for secure communications between Control Centers.	
Likes 0	
Dislikes 0	
Response	
Heather Morgan - EDP Renewables North America LLC - 5	
Answer	No
Document Name	
Comment	
Generator Operator Control Centers are required to follow specifications pursuant to the requirements outlined by RCs, ISO,s RTOs, BAs, and TOPs. To ensure GOP's are able to properly carry out requirements for all of these parties and CIP-012-2, CIP-012-2's Implementation Plan should be phased in similar to IRO-010, and TOP-003. Otherwise, GOP Control Centers will not be able to properly plan for any requirements delivered by the interconnecting authorities as a result of this Standard.	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	No
Document Name	
Comment	
Request changing 12 months to 18 months in the implentation plan to allow time to make any required changes including design, procurement, CIP assesment and deployment.	
Likes 0	
Dislikes 0	
Response	
Aaron Austin - AEP - 3	
Answer	No

Document Name	
Comment	
AEP suggests that the implementation time frame should be extended to at least 24 months to allow for activities such as coordination, budgeting, procurement, implementation and testing.	
Likes 0	
Dislikes 0	
Response	
Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	No
Document Name	
Comment	
NRECA asserts that smaller entities may need to procure equipment and implement technical controls that are not currently in place. The implementation of the plan(s) detailed in requirement R1 could be impacted by budget cycles, procurement processes, and third party vendor availability. NRECA recommends that the implementation plan be revised to allow 12 months for the development of the plan in requirement R1 and 24 months for the implementation.	
Likes 0	
Dislikes 0	
Response	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	No
Document Name	
Comment	
Hydro Québec is in agreement with TFIST's comments below in regards to taking into consideration technical complexities and coordination between entities; however we suggest that the documented plan in R1 include an implementation plan with deadlines not exceeding 36 months, rather than a prescribed delay for implementing R2. Furthermore, clarifications are requested in regards to the question"please note the actions you will take that require this amount of time to complete. 1. The time to implement R1 (develop plan) could be 12 months from time of order. For implementation of R2 there should be an additional 24 months allowed to undertake implementation. This would include identifying all links and protections, with changes needed to address communications service contracts and related relationships to adjust for new protections. This would also involve inventory of data to comply with identification of all data transmitted between control centers.	

2. Due to technical complexity, agreements (outsourced and between Entities), procurement, contracts and coordination between Entities (and provisioning of private networks), request that the SDT consider:

a)a phased implementation over a five or longer year period, or b) to avoid impacting reliability, that existing contracts, equipment, etc stay in place. New contracts / equipment will need to follow this new Standard.

Likes 0	
Dislikes 0	

Response

Lona Calderon - Salt River Project - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

SRP requests 24 calendar months due to the complex details and logistics associated with implementation. The Impact from encryption is unknown. Because the data is being sent in real-time, it is difficult to test how encryption will affect reliability.

More research and evaluation is required to understand the implications encryption will have as it may require architecture changes to account for the extra computing resources required. Additionally, time is required to budget for funds in order to support any required infrastructure improvements required.

Likes 0	
Dislikes 0	

Response

Thomas Breene - WEC Energy Group, Inc. - 3

Answer	No
Document Name	

Comment

The 12 month time period may only work for Entities who are vertically intergraded. The flow of applicable BES data within CIP-012-1 can be viewed as a “spider web” of data transfer for large RC foot-prints. With this being said, there may be non-compliance issues when one side of the data transference is protected and the other side is not. The SDT should propose a phased in approach to protecting data. A five (5) year implementation plan will allow entities to fund these projects. This is especially import to small entities. Per the NERC Guidance concerning “Phase Implementation Plans with Completion Percentages (http://www.nerc.com/pa/comp/guidance/CMEPPracticeGuidesDL/CMEP_Practice_Guide_Phased_Implementation_Completion_Percentages.pdf) please state that the CIP-012-1 does not fall under this guidance.

Likes 0	
Dislikes 0	

Response	
Russell Noble - Cowlitz County PUD - 3	
Answer	No
Document Name	
Comment	
Cowlitz PUD supports the comments submitted by APPA.	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	No
Document Name	
Comment	
We recommend at least 18 months due to the quantity of details and logistics.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Con-Edison and Dominion	
Answer	No
Document Name	
Comment	
· The time to implement R1 (develop plan) could be 12 months from time of order. For implementation of R2 there should be an additional 24 months allowed to undertake implementation. This would include identifying all links and protections, with changes needed to address communications service contracts and related relationships to adjust for new protections. This would also involve inventory of data to comply with identification of all data transmitted between control centers. · Due to technical complexity, agreements (outsourced and between Entities), procurement, contracts and coordination between Entities (and provisioning of private networks), request that the SDT also consider the following option for R2 implementation:	

a. a phased implementation over a five or longer year period, or

b. to avoid impacting reliability, existing contracts, equipment, etc. be grandfathered until new / replacements are in place.

Likes 0	
Dislikes 0	

Response

Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2

Answer	No
Document Name	

Comment

ERCOT ISO signs on to the ITC SWG comments:

The ITC SWG also encourages the drafting team to make the requirement forward-looking in regards to contracts currently in place. Provisions should be set for legacy contracts including grandfathering of existing agreements and equipment. Implementation of controls involving telecommunications providers will require coordination and scheduling to align to the providers' resource availability and reduce adverse impact on reliability. This should not require renewal and renegotiation of existing contracts until they reach the end of the existing contract period.

It should be noted that it is difficult to determine suitability of the implementation timeline when there are open questions about the viability of available solutions for adequate protections.

More time is necessary to allow for coordination with a large number of parties. This will require budgeting, planning, and scheduling with external resources for implementation. It will also require significant testing and validation by parties on both ends of a connection.

The ITC SWG recommends a phased implementation with defined milestones similar to CIP-014. Consider the following:

- For creation of the plan, 12 months should be allowed to (1) conduct an impact assessments, (2) identify the approach to be included in the plan, (3) implementation milestones, and (4) implementation schedule. This could identify the communication links that have protections currently in place. The plan could also include identifying all links and protections requiring changes to address service contracts and related relationships to adjust for new protections. The plan could then be approved by an appropriate entity.

- For implementation of the plan, additional time should be allowed for budgeting, planning, and scheduling with external resources. This includes planning with other Responsible Entities as well as telecommunications providers.

Likes 0	
Dislikes 0	

Response

Shelby Wade - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company

Answer	No
Document Name	
Comment	
We support SERC's comments.	
Likes 0	
Dislikes 0	
Response	
Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 3	
Answer	No
Document Name	
Comment	
Tacoma Power supports the comments of APPA	
Likes 0	
Dislikes 0	
Response	
Theresa Rakowsky - Puget Sound Energy, Inc. - 1	
Answer	No
Document Name	
Comment	
PSE believes a 24 month implementation period and/or phased implementation approach is appropriate due to required coordination between registered entities, potential need for renegotiation of contracts and/or agreements with other entities, and potential for significant technical complexity for implementation.	
Likes 0	
Dislikes 0	
Response	
Jack Cashin - American Public Power Association - 4	
Answer	No

Document Name	
Comment	

APPA does not agree with the implementation proposal timeline. The time to implement R1 (develop a plan) should be 12 months from the time of the order.

Due to technical complexity, agreements (outsourced and between registered entities), procurement, contracts and coordination between registered entities (and provisioning of private networks), APPA requests that the SDT consider the following options for R2 implementation:

• additional 24 months allowed to undertake implementation,

• using a phased implementation over a five or longer year period

- in recognition that there is the potential for several existing contracts will have to be replaced (and associated equipment) that affected contracts be grandfathered until new and or, replacements can be put in place.

Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	

CenterPoint Energy recommends the effective date for CIP-012-1 to be 24 months after FERC approval. For instances where applicable data is being transmitted between Control Centers owned by two or more separate Responsible Entities, additional time is needed to coordinate plans and develop agreements to ensure adequate protection is applied.

Likes 0	
Dislikes 0	
Response	
Warren Cross - ACES Power Marketing - 1,3,4,5 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standards Collaborators	
Answer	No
Document Name	
Comment	

New entities that are impacted by the new definition should be treated as “newly identified CIP facilities” and should be given the standard 18 month implementation period. Not the proposed 12 month implementation period. Budgetary cycles would need to be considered and an additional reason for the 18 months.

Likes 0	
Dislikes 0	

Response

Sheranee Nedd - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs

Answer	No
Document Name	

Comment

PSEG Supports the NPCC comments.

Likes 1	PSEG - PSEG Fossil LLC, 5, Kucey Tim
Dislikes 0	

Response

Michael Puscas - ISO New England, Inc. - 2

Answer	No
Document Name	

Comment

The time to implement the first requirement (develop plan) could be 12 months from time of order. For implementation of the plan, however (R2) there should be an additional 12 months allowed to undertake implementation. This would include identifying all links and protections, with changes needed to address communications service contracts and related relationships to adjust for new protections.

Likes 0	
Dislikes 0	

Response

David Greyerbiehl - CMS Energy - Consumers Energy Company - 5

Answer	No
Document Name	

Comment

Twelve calendar months for implementation may not be sufficient, twenty-four calendar months should be recommended.

Likes 0	
Dislikes 0	

Response

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

BPA requests clarification about what “Physically protecting the communication links transmitting the data” in section 1.1 means. If it means protecting the data at the source (at the Control Center), the implementation period is acceptable. BPA will be required to update customer agreements during the implementation period.

If it means the data must be protected throughout the transmission, it would seem that could only be accomplished with encryption. For cases where the existing equipment is not capable of encryption, BPA cannot propose an implementation timeline or solution other than technically feasible exception.

Likes 0	
Dislikes 0	

Response

James Anderson - CMS Energy - Consumers Energy Company - 1

Answer	No
Document Name	

Comment

Twelve calendar months for implementation may not be sufficient, twenty-four calendar months should be recommended.

Likes 0	
Dislikes 0	

Response

Brian Evans-Mongeon - Utility Services, Inc. - 4

Answer	No
Document Name	

Comment
Utility Services does not agree with the implementation proposal timeline. The time to implement R1 (develop a plan) should be 12 months from the time of the order. Due to technical complexity, agreements (outsourced and between registered entities), procurement, contracts and coordination between registered entities (and provisioning of private networks), UTILITY SERVICES requests that the SDT consider the following options for R2 implementation: · additional 24 months allowed to undertake implementation, · using a phased implementation over a five or longer year period, or · in recognition that there is the potential for several existing contracts will have to be replaced (and associated equipment) that affected contracts be grandfathered until new and or, replacements can be put in place.

Likes 0	
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No
Document Name	

Comment
Southern Company feels that 12 months is not enough time to implement the Standard as currently written. Implementation of the proposed methods of compliance could embark entities on budget and procurement processes to acquire new, upgraded, or revamped hardware, software, or other physical components at existing sites, and this can be a lengthy process. Southern recommends at least a 24 month or greater implementation timeframe. Southern agrees with comments provided by other commenters that the complexity of the technology solutions to be implemented, the number of interconnecting lines to secure, connection point testing, and coordination requirements with external stakeholders are additional factors supporting a 2 year implementation period.

Likes 0	
Dislikes 0	

Response

Ronald Donahey - TECO - Tampa Electric Co. - 3	
Answer	No
Document Name	

Comment
If additional contracts/agreements are required to address a plan for other entities, Registered Entities may need a longer time to implement the plan (Requirement R2). Tampa Electric Company recommends an 18 month timeframe for Requirement 2.

Likes 0	
Dislikes 0	

Response

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group

Answer	No
Document Name	

Comment
The Standard Review Group has a concern that all Implementation needs may not be met in a timely fashion at the twelve (12) calendar month time frame. We would recommend that the drafting team extends the deadline to eighteen (18) calendar months. Due to technological changes needed to secure the data and collaboration between sending and receiving party, we feel more time is needed to implement the standard.

Likes 0	
Dislikes 0	

Response

Wendy Center - U.S. Bureau of Reclamation - 5

Answer	No
Document Name	

Comment
Eighteen calendar months after the approval of the control center definition and the CIP-012-1 standard to allow entities time to evaluate the impact of the changes effected by the new standard and implement an appropriate response.

Likes 0	
Dislikes 0	

Response

James Gower - Entergy - NA - Not Applicable - SERC

Answer	No
Document Name	

Comment
Cannot support at this time until additional clarity is given to requirements for written communications outside of operational data and for Operational Planning Analysis data. If corporate systems require protection that could greatly affect implementation timelines. Additionally, the twelve month window may fall outside of yearly budget planning, compressing project planning timelines.

Likes 0	
Dislikes 0	

Response

Mark Riley - Associated Electric Cooperative, Inc. - 1	
Answer	No
Document Name	

Comment
AECI asserts that smaller entities may need to procure equipment and implement technical controls that are not currently in place. The implementation of the plan(s) detailed in requirement R1 could be impacted by budget cycles, procurement processes, and third party vendor availability. AECI recommends that the implementation plan be revised to allow 12 months for the development of the plan in requirement R1 and 24 months for the implementation

Likes 0	
Dislikes 0	

Response

Guy Andrews - Georgia System Operations Corporation - 4	
Answer	No
Document Name	

Comment
• Additional time would be required to plan, budget, and implement this Standard. Further, only allowing 12 months for implementation may limit the technology solutions that may be implemented to only those that can be accomplished with minimal planning and testing. GSOC requests twenty-four months.

Likes 0	
Dislikes 0	

Response

Annette Johnston - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	No

Document Name	
Comment	
At least three years is needed in order to coordinate with other entities, including specification, design, budgeting, implementation and testing.	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	
Comment	
See MidAmerican Energy Company comments.	
Likes 0	
Dislikes 0	
Response	
Haley Sousa - Public Utility District No. 1 of Chelan County - 5	
Answer	No
Document Name	
Comment	
The coordination time required to perform a migration to secure communications protocols is expected to take longer than the schedule presented by the SDT. CHPD recommends at least twenty-four (24) calendar months to implement communication updates and implement other available protection measures.	
Likes 0	
Dislikes 0	
Response	
Janis Weddle - Public Utility District No. 1 of Chelan County - 6	
Answer	No
Document Name	

Comment
The coordination time required to perform a migration to secure communications protocols is expected to take longer than the schedule presented by the SDT. CHPD recommends at least twenty-four (24) calendar months to implement communication updates and implement other available protection measures.

Likes 0	
Dislikes 0	

Response

sean erickson - Western Area Power Administration - 1

Answer	No
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

David Greene - SERC Reliability Corporation - 10, Group Name SERC CIPC

Answer	No
Document Name	3B-2016-02_CIP-012-1_Unofficial_Comment_Form_CIPC.docx

Comment

Likes 0	
Dislikes 0	

Response

Lauren Price - American Transmission Company, LLC - 1

Answer	No
Document Name	

Comment

Likes 0

Dislikes 0	
Response	
Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
A region-wide agreement may be difficult to develop and execute in a year. Tri-State believes 18 months would be more appropriate.	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE	
Answer	Yes
Document Name	
Comment	
Xcel Energy believes that the Implementation Plan would allow sufficient time for our operating companies to implement required controls specified in the language of CIP-012-1. However, Xcel Energy would require coordination from up to 25 other Responsible Entities is communicates BES data with and cannot speak to their abilities. Any agreements in coordination between entities would need to go through a legal review process, which could take more than 12 months to formalize and implement. A 24 month implementation period may be more feasible given the legal review challenges that would inevitably occur.	
Likes 0	
Dislikes 0	
Response	
David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
OPG has some concerns and recommends a graded approach implementation over a longer period of time. The communications links requiring protections will require inventory; this will be a complex task for the RC.	

The recommended 12 months may be sufficient for the inventory, however we also need to determine the applicable solution and agree on the solution with another entities.	
Likes 0	
Dislikes 0	
Response	
Laura McLeod - NB Power Corporation - 5	
Answer	Yes
Document Name	
Comment	
See 1 above. Note that additional time may be required to reach consensus between entities when establishing security protocols.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb On Behalf of: Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 3, 5, 1, 6; James McBee, Great Plains Energy - Kansas City Power and Light Co., 3, 5, 1, 6; Jessica Tucker, Great Plains Energy - Kansas City Power and Light Co., 3, 5, 1, 6; Jim Flucke, Great Plains Energy - Kansas City Power and Light Co., 3, 5, 1, 6; - Douglas Webb	
Answer	Yes
Document Name	
Comment	
The company will review current systems and protections to identify if further action is required to protect the communications links between control centers as set forth in the approved Standard.	
Likes 0	
Dislikes 0	
Response	
RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dermot Smyth - Con Ed - Consolidated Edison Co. of New York - 5, Group Name Con Edison	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Philip Huff - Arkansas Electric Cooperative Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Shannon Fair - Colorado Springs Utilities - 1,3,5,6, Group Name Colorado Springs Utilities	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alice Wright - Arkansas Electric Cooperative Corporation - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Shaw - Lower Colorado River Authority - 1, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Laurie Williams - PNM Resources - Public Service Company of New Mexico - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	
Document Name	
Comment	
The California ISO supports the comments of the Security Working Group (SWG).	
Likes 0	
Dislikes 0	
Response	

Kristine Ward - Seminole Electric Cooperative, Inc. - 1,2,4,5,6 - FRCC	
Answer	
Document Name	
Comment	
SECI would like examples of evidence so we know how to proceed	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
This question implies there are NERC Glossary terms in the Implementation Plan. There are no NERC Glossary terms in the CIP-012-1 Implementation Plan. Texas RE does not oppose the enforcement timelines set forth in the proposed Implementation Plan. However, Texas RE respectfully requests that the SDT provide a specific justification for any proposed implementation timeframes, as well as any revisions to the timeframes as currently proposed. The goal is to ensure there are no issues with the implementation plan such as not having an initial performance date where one is needed or not including information for new facilities such as the instance that led to an errata change in the PRC-023-4 implementation plan. These issues cause confusion and ambiguity for both registered entities and Regional Entities upon enforcement of the standard.	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 3, Group Name FirstEnergy Corporation	
Answer	
Document Name	
Comment	
FirstEnergy recommends adjusting the Implementation Plan time period to become effective the first day of the first calendar quarter that is eighteen (18) calendar months after the effective date of the applicable governmental authority's order approving the standard. The	

additional time will be needed to ensure that the implementation of any new technology (e.g. encryption) does not impact reliability of the BES.

Likes 0	
Dislikes 0	

Response

4. The SDT believes proposed CIP-012-1 provides entities with flexibility to meet the reliability objectives in a cost effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost effective approaches, please provide your recommendation and, if appropriate, technical justification.

Janis Weddle - Public Utility District No. 1 of Chelan County - 6	
Answer	No
Document Name	
Comment	
CHPD cannot determine if the objectives may be accomplished in a cost-effective manner until further clarification is provided for physical or other equally effective protection measures and the request for electronic mail exclusion is added. CHPD also has concerns with vendor availability, with respect to the system software implementation that will be required for all entities industry-wide. The comments provided by other entities to develop an industry-wide encryption specification is appealing and CHPD believes that would provide a better method for achieving the desired intra-entity security.	
Likes 0	
Dislikes 0	
Response	

Haley Sousa - Public Utility District No. 1 of Chelan County - 5	
Answer	No
Document Name	
Comment	
CHPD cannot determine if the objectives may be accomplished in a cost-effective manner until further clarification is provided for physical or other equally effective protection measures and the request for electronic mail exclusion is added. CHPD also has concerns with vendor availability, with respect to the system software implementation that will be required for all entities industry-wide. The comments provided by other entities to develop an industry-wide encryption specification is appealing and CHPD believes that would provide a better method for achieving the desired intra-entity security.	
Likes 0	
Dislikes 0	
Response	

Laura McLeod - NB Power Corporation - 5	
Answer	No
Document Name	
Comment	

See 2 above.	
Likes 0	
Dislikes 0	
Response	
James Gower - Entergy - NA - Not Applicable - SERC	
Answer	No
Document Name	
Comment	
Cannot agree with the flexibility and cost effectiveness until additional clarity is given to requirements for written communications outside of operational data and Operational Planning Analysis. If corporate systems require protection that could greatly affect potential cost.	
Likes 0	
Dislikes 0	
Response	
Ronald Donahey - TECO - Tampa Electric Co. - 3	
Answer	No
Document Name	
Comment	
Until industry is able to determine the extent of information to be protected extends beyond the real-time 15 minute time frame, we are not able to agree with the statement regarding cost-effective manner.	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No
Document Name	
Comment	

The cost of implementing the intended protections, as they are understood by Southern, will be prohibitive. See the response to Question 1 as the primary driver for our disagreement with this question, as well as other supporting information provided in response to Question 3.

Likes 0	
Dislikes 0	

Response

James Anderson - CMS Energy - Consumers Energy Company - 1

Answer	No
Document Name	

Comment

More flexibility and less guidance could lead to inconsistency on requirement implementation among different entities.

Likes 0	
Dislikes 0	

Response

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

If it means the data must be protected throughout the transmission, it would seem that could only be accomplished with encryption. For cases where the existing equipment is not capable of encryption, replacement will be costly and implementation lengthy.

Likes 0	
Dislikes 0	

Response

David Greyerbiehl - CMS Energy - Consumers Energy Company - 5

Answer	No
Document Name	

Comment

More flexibiity and less guidance could lead to inconsistency on requirement implentation among different entities.

Likes 0	
Dislikes 0	

Response

Michael Puscas - ISO New England, Inc. - 2

Answer	No
Document Name	

Comment

To fully assess the logistics and costs associated with compliance, some guidance or specification of boundaries of communications links involved would be required for entities to complete assessment of impacts to their operations.

Likes 0	
Dislikes 0	

Response

Warren Cross - ACES Power Marketing - 1,3,4,5 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standards Collaborators

Answer	No
Document Name	

Comment

(1) The standard doesn't directly address the Inter-Control Center Communications Protocol (ICCP) for exchanging data between control centers or utilities. Will those ICCP servers and supportive infrastructure need to be upgraded or replaced with data encryption capabilities to support compliance with this standard?

(2) The standard doesn't provide any direction as to what is the level of physical and logical protection that is mandatory. We ask the SDT to develop guidance to clarify this ambiguity and identify how all entities can achieve a minimum level of compliance.

Likes 0	
Dislikes 0	

Response

Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2

Answer	No
Document Name	
Comment	

ERCOT ISO signs on to the ITC SWG comments:

In addition to the comments provided in response to question 3, the SWG offers these comments regarding cost effectiveness. Open Source options to satisfy the requirement to protect communication links and sensitive bulk electric system data communicated between bulk electric systems Control Centers are limited. Few options generally translated to high vendor leverage, which could lead to high implementation costs. It is unclear how or whether costs could be shared among participants in the network. Architectural changes to support these requirements should be spread out over several years. Plus there will be business impacts.

Likes 0	
Dislikes 0	
Response	

Lona Calderon - Salt River Project - 1,3,5,6 - WECC

Answer	No
Document Name	
Comment	

SRP needs more detail on what would be acceptable as physical security to determine if the standard provides adequate flexibility. Also, as stated in response to question 3, significant capital may need to be budgeted in order to implement architecture improvements to address the required computing resources for encrypting and decrypting of data. Additionally, SRP agrees with LPPC's comment that an industry-wide initiative for an encryption specification may be a more cost-effective approach than a new standard.

Likes 0	
Dislikes 0	
Response	

Aaron Austin - AEP - 3

Answer	No
Document Name	
Comment	

AEP believes that most entities are at the mercy of what Balancing Authorities and Reliability Coordinators will require. This coupled with the fact that data for Operational Planning and Analysis is included, flexibility may lead to variability and as such makes it only a presumption that solutions will be cost effective.

Likes 0	

Dislikes 0	

Response

Dennis Sismaet - Northern California Power Agency - 6

Answer	No
Document Name	

Comment

NCPA does not agree that the standard provides entities with the flexibility to implement the standard cost-effectively and offers these further suggestions. To fully assess the logistics and costs associated with compliance, some guidance or specification of boundaries of communications links involved would be required for entities to complete assessment of impacts to their operations. In addition, architectural changes should be spread out over several budget cycles (years).

Likes 0	
Dislikes 0	

Response

Marty Hostler - Northern California Power Agency - 5

Answer	No
Document Name	

Comment

NCPA does not agree that the standard provides entities with the flexibility to implement the standard cost-effectively and offers these further suggestions. To fully assess the logistics and costs associated with compliance, some guidance or specification of boundaries of communications links involved would be required for entities to complete assessment of impacts to their operations. In addition, architectural changes should be spread out over several budget cycles (years).

Likes 0	
Dislikes 0	

Response

Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body

Answer	No
Document Name	

Comment

See APPA Comments.

Likes 0	
Dislikes 0	
Response	
Alice Wright - Arkansas Electric Cooperative Corporation - 4	
Answer	No
Document Name	
Comment	
See attachment	
Likes 0	
Dislikes 0	
Response	
Philip Huff - Arkansas Electric Cooperative Corporation - 3	
Answer	No
Document Name	
Comment	
Please see our comments to Question 1. The additional flexibility in this context has the potential to cause more confusion when selecting a mechanisms to secure the data.	
Likes 0	
Dislikes 0	
Response	
David Rivera - New York Power Authority - 3	
Answer	No
Document Name	
Comment	
1. To fully assess the logistics and costs associated with compliance, some guidance or specification of boundaries of communications links involved would be required for entities to complete assessment of impacts to their operations. 2. Architectural changes should be spread out over several budget cycles (years). Plus there will be business impacts. See comments to Q3	
Likes 0	

Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	No
Document Name	

Comment

In addition to the comments provided in response to question 3, the IESO offers these comments regarding cost effectiveness. Open Source options to satisfy the requirement to protect communication links and sensitive bulk electric system data communicated between bulk electric systems Control Centers are limited. Few options generally translated to high vendor leverage, which could lead to high implementation costs. It is unclear how or whether costs could be shared among participants in the network. Architectural changes to support these requirements should be spread out over several years. Plus there will be business impacts.

Likes 2	Hydro One Networks, Inc., 1, Farahbakhsh Payam; Hydro One Networks, Inc., 3, Malozewski Paul
Dislikes 0	

Response

Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino

Answer	No
Document Name	

Comment

It may be more cost effective if an industry wide initiative is conducted with encryption specifications.

Likes 0	
Dislikes 0	

Response

Laura Nelson - IDACORP - Idaho Power Company - 1

Answer	No
Document Name	

Comment	
There will likely be additional costs associated with administrative overhead, hardware, and software, as well as costs associated with monitoring the performance of the implemented solutions.	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	No
Document Name	
Comment	
TVA suggests additional guidance is needed to identify examples of acceptable standard security mechanisms for exchanging data between entities. Without clearer guidance some entities may out of an abundance of caution spend beyond what is necessary to mitigate this risk, or expend unnecessary effort determining a mutual security mechanism.	
Likes 0	
Dislikes 0	
Response	
Lauren Price - American Transmission Company, LLC - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	Yes
Document Name	
Comment	

See MidAmerican Energy Company comments.	
Likes 0	
Dislikes 0	
Response	
Annette Johnston - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	Yes
Document Name	
Comment	
The three bullets are constructive.	
Likes 0	
Dislikes 0	
Response	
Guy Andrews - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
no comments	
Likes 0	
Dislikes 0	
Response	
David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
OPG recommends further collaboration to further enhance the cost effectiveness. Solution implementation will require collaboration when the communication link is between CC belonging to different entities. There is also the issue of agreed solution; for example the stronger the protection	

implemented the higher the budgetary costs. If this may not be an issue for the RC it can be an issue for a small entity required to report to the RC via these communication links.	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Utility Services agrees that the standard provides entities with the flexibility to implement the standard cost-effectively and offers these further suggestions. To fully assess the logistics and costs associated with compliance, some guidance or specification of boundaries of communications links involved would be required for entities to complete assessment of impacts to their operations. In addition, architectural changes should be spread out over several budget cycles (years).	
Likes 0	
Dislikes 0	
Response	
Sheranee Nedd - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	
PSEG supports the NPCC comments.	
Likes 1	PSEG - PSEG Fossil LLC, 5, Kucey Tim
Dislikes 0	
Response	
Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 3	
Answer	Yes
Document Name	
Comment	

Tacoma Power supports the comments of APPA	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Con-Edison and Dominion	
Answer	Yes
Document Name	
Comment	
· To fully assess the logistics and costs associated with compliance, some guidance or specification of boundaries of communications links involved would be required for entities to complete assessment of impacts to their operations. · Architectural changes should be spread out over several budget cycles (years), and there will be business impacts. See comments to Q3	
Likes 0	
Dislikes 0	
Response	
Russell Noble - Cowlitz County PUD - 3	
Answer	Yes
Document Name	
Comment	
Cowlitz PUD supports the comments submitted by APPA.	
Likes 0	
Dislikes 0	
Response	
Thomas Breene - WEC Energy Group, Inc. - 3	
Answer	Yes
Document Name	
Comment	

Thank you for adding the third bullet of R1.

Likes 0	
Dislikes 0	

Response

Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1

Answer	Yes
Document Name	

Comment

1. To fully assess the logistics and costs associated with compliance, some guidance or specification of boundaries of communications links involved would be required for entities to complete assessment of impacts to their operations.
2. Architectural changes should be spread out over several budget cycles (years). Plus there will be business impacts. See comments to Q3.

Likes 0	
Dislikes 0	

Response

Heather Morgan - EDP Renewables North America LLC - 5

Answer	Yes
Document Name	

Comment

None at this time

Likes 0	
Dislikes 0	

Response

Vivian Vo - APS - Arizona Public Service Co. - 3

Answer	Yes
Document Name	

Comment

While the Standard is sufficiently flexible for an individual responsible entity, it leaves a potential chasm between different entities' interpretation of cost-effective approaches. A top-tier utility's impression of a cost effective approach may not match a smaller neighbor's idea of a cost effective approach. Such a disparity could encumber both large and small entities with disparate concerns that complicate negotiation and agreement on appropriate solutions.

Likes 0	
Dislikes 0	

Response

Chris Scanlon - Exelon - 1

Answer	Yes
Document Name	

Comment

Exelon agrees with the approach used in CIP-012-1, which allows each Registered Entity to analyze risk and use discretion in determining the best risk mitigation implementation for protecting transmission of applicable data.

Likes 0	
Dislikes 0	

Response

Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	Yes
Document Name	

Comment

Thank you for adding the third bullet of R1

Likes 0	
Dislikes 0	

Response

Dermot Smyth - Con Ed - Consolidated Edison Co. of New York - 5, Group Name Con Edison

Answer	Yes
Document Name	

Comment

To fully assess the logistics and costs associated with compliance, some guidance or specification of boundaries of communications links involved should be provided so that entities can perform an assessment of impacts to their operations.

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 agrees that the language provided in R1 appears to provide a Responsible Entity flexibility in how it may implement the standard, but concern exists in the amount of protection options given. Additional documentation such as Implementation Guidance including additional suggestions for implementation may give entities more options to consider, while still keeping the flexibility of determining what is the most suitable method of protection for said entity.

Likes 0	
Dislikes 0	

Response

Douglas Webb - Douglas Webb On Behalf of: Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 3, 5, 1, 6; James McBee, Great Plains Energy - Kansas City Power and Light Co., 3, 5, 1, 6; Jessica Tucker, Great Plains Energy - Kansas City Power and Light Co., 3, 5, 1, 6; Jim Flucke, Great Plains Energy - Kansas City Power and Light Co., 3, 5, 1, 6; - Douglas Webb

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Laurie Williams - PNM Resources - Public Service Company of New Mexico - 1

Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Shaw - Lower Colorado River Authority - 1, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
David Greene - SERC Reliability Corporation - 10, Group Name SERC CIPC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Theresa Rakowsky - Puget Sound Energy, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Shelby Wade - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 3, Group Name FirstEnergy Corporation	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Poston - Santee Cooper - 3, Group Name Santee Cooper	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Shannon Fair - Colorado Springs Utilities - 1,3,5,6, Group Name Colorado Springs Utilities	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Hohenshilt - Talen Energy Marketing, LLC - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donald Lock - Talen Generation, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Frank Pace - Central Hudson Gas & Electric Corp. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
George Brown - Acciona Energy North America - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jack Cashin - American Public Power Association - 4	
Answer	
Document Name	
Comment	
APPA agrees that the standard provides entities with the flexibility to implement the standard cost-effectively and offers these further suggestions. To fully assess the logistics and costs associated with compliance, some guidance or specification of boundaries of communications links involved would be required for entities to complete assessment of impacts to their operations. In addition, architectural changes should be spread out over several budget cycles (years).	
Likes 0	

Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE does not have comments on this questions.	
Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	
Document Name	
Comment	
The California ISO supports the comments of the Security Working Group (SWG).	
Likes 0	
Dislikes 0	
Response	

5. If you have additional comments on the proposed CIP-012-1 – Cyber Security -- Communication Networks drafted in response to the FERC directive that you have not provided in response to the questions above, please provide them here.

Richard Vine - California ISO - 2

Answer	
Document Name	

Comment

The California ISO supports the comments of the Security Working Group (SWG).

Likes 0	
Dislikes 0	

Response

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority

Answer	
Document Name	

Comment

TVA notes that the requirement language focuses on the risk of unauthorized disclosure or modification of data. In an operational environment the integrity and availability legs of the CIA triad are more critical than the confidentiality. TVA suggests consider revising to focus on ensuring the integrity and availability of the data.

Likes 0	
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion

Answer	
Document Name	

Comment

Applicability:

Based on the first 2 questions in the proposed RSAW requiring entities to prove that the standard does not apply to them, could the Applicability section of the standard be modified to indicate that the standard only applies to those specific registered entities (e.g., GOPs and TOs) that maintain Control Centers AND transmit data between Control Centers?

Additionally, the proposed standard does not provide a sufficient level of detail on how entities should work together to handle security concerns across a communication network. The standard should clearly identify where the obligations for protecting data in a communication network start and end per entity.

Technical Rationale:

Does the TO field asset box on page # 5 of Technical Rationale and Justification for CIP-012-1 document include TO Control Centers? If no, where are TO Control Centers represented ?

Implementation Guidance:

CIP-012 R2 requires the Responsible Entity to implement on or more documented plan(s) to mitigate the risk of the unauthorized disclosure or modification of applicable data whish being transmitted between Control Centers. Without implementation guidance describing how to accomplish this risk mitigation either physically protecting the communication links transmitting the data or logically protecting the data during transmission; or some other equally effective means it is difficult to predict the amount of time that would be required to implement this requirement part and therefore we cannot assume the 12 months prescribed in the proposed implementation plan is adequate.

Likes 0	
Dislikes 0	

Response

Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC

Answer	
Document Name	

Comment

If the region is responsible for the system, what does the entity have to do for compliance? All entities would have to coordinate with the region on a solution. The solution may require additional equipment to be installed. A region-wide formal agreement may be difficult to develop and execute in a year.

Likes 0	
Dislikes 0	

Response

Anthony Jablonski - ReliabilityFirst - 10

Answer	
Document Name	

Comment

Even though ReliabilityFirst votes in the affirmative, ReliabilityFirst provides the following comments for consideration:

1. Requirement R2

i. Requirement R2 of the Standard does not identify a “reasonable” timeline for implementing the plan identified in R1. This lack of time determinant could lead to prolonged and needless delay in implementing the required protections.

ii. Requirement R2 uses the phrase “CIP Exceptional Circumstances”. The intent is “to protect confidentiality and integrity of data transmitted between Control Centers required for reliable operation of the Bulk Electric System (BES).”

ReliabilityFirst questions if using the phrase “CIP Exceptional Circumstances” is appropriate here. The definition of 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.” ReliabilityFirst believes CIP Exceptional Circumstances criteria are not relative to data transmission.

Likes 0	
Dislikes 0	

Response

George Brown - Acciona Energy North America - 5

Answer	
Document Name	

Comment

1- Generator Operators within the ERCOT footprint who are not also a Qualified Scheduling Entity (QSE) will not be able to comply with the standard as written if their Control Center transmits and receives the data as specified in Requirement R1.

Within the ERCOT footprint the sensitive BES data transmitted between the Control Centers of the Balancing Authority (BA), Transmission Operator (TOP), Reliability Coordinator (RC) and Generator Operator (GOP) is submitted through the QSE (Assume that ERCOT is acting as the RC, BA and/or TOP for particular GOP and that GOP is not also a QSE). The QSE is not a recognized NERC Functional Entity and as such would not be subject to adhering to NERC Reliability Standards. Therefore it would not be possible for a GOP to protect the sensitive BES data that is transmitted to and from the Control Center of the QSE and ERCOT that ultimately is either being sent or received by the GOP Control Center. NERC CIP-012-1, as written, does not account for this ERCOT nuance.

2 - Pursuant to NERC CIP-012-1, §4 Applicability, this standard is applicable to the Generator Owner. However, the proposed definition of Control Center, exempts the Generator Owner as it only speaks to the Generator Operator’s Control Center. NERC CIP-012-1 should not be applicable to the Generator Owner.

Likes 0	
Dislikes 0	

Response

Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of

Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino	
Answer	
Document Name	
Comment	

We seek clarification in the standard verbiage that the intent of this standard applies to inter control center communication. In addition, it would be beneficial to have guidance on key management and inter utility agreements particularly as it pertains to coordination for encryption of data between 3rd parties and compliance impacts on reliability.

Likes 0	
Dislikes 0	
Response	

Leonard Kula - Independent Electricity System Operator - 2	
Answer	
Document Name	
Comment	

The IESO asserts that the proposed standard does not make clear how entities should work together when addressing security concerns across a communication network link. If both entities work with CIP Standard assumptions on both ends of a communication network, some support for joint handling of issues could be made clear. However, if only one entity is CIP-compliant for a given link, the current standard draft does not make clear the extent of protection expected for the data. The Standard should provide more information on the ownership of obligations for protecting the entire link

It is unclear whether the addition of CIP-012 affects the exemptions of communication networks in any of the applicability sections of other standards (CIP-002 through CIP-011). The IESO requests clarification that CIP-012 fills in some of the gap created the CIP-002 – CIP-011 third party telecommunications exemption (4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.)

It has been ten years since the SANDIA report ("Secure ICCP Considerations and Recommendations"), the only detailed report on this subject which could be considered close having entered mainstream awareness in the industry. Today, as ten years ago, Secure ICCP is not a viable choice for utilities, if only due to limited community experience and vendor support, not to mention the complexities of key management. The transition strategies that SANDIA discusses – Layer 3 protection using IPsec and Layer 2 protection with hardware encryption – remain today's target solutions.

IPsec is a viable alternative. Over MPLS, IPsec could secure GRE tunnels between CE routers. Challenges with this approach include the possibility of having to hire a third party to manage certificates and IPsec links, especially for ISOs that do not manage their own MPLS networks.

The IESO position on security architecture is that business transactions (such as ICCP) should not be tightly coupled with encryption technologies. Solutions should prefer network overlays versus security extensions to a protocol (such as Secure ICCP or DNP3 SA).

The security architecture should prefer least-latent encryption solutions at the Ethernet or IP layers of the network stack. MACsec (802.1AE) models the spirit of an optimal solution within a metro area – could it scale wider?

The IESO's overall position on Secure ICCP is that it represents too much reliability risk. The IESO is concerned about the lack of open standards and protocols available to meet the confidentiality and integrity security objectives of CIP-012. Assuming that a solution involves encryption, the only two

open standards and protocols that can meet the CIP-012 security objectives are IPsec and TLS. The potential for vendor leverage in such a small open solution space is large. Vendor-managed MPLS networks, typical among utilities, already entrench high annual telecommunication costs in utility budgets. Security vendors continue to benefit from the expense of establishing layered cyber defenses. Open Source solutions provide a cost and agility refuge from this lopsided value chain without compromising defense layers. The trend toward managed services makes the cost problem worse for utilities, especially in the context of insufficiently evaluated risk. Vendor leverage only grows given the practical consideration that all the communicating parties in a WAN of connected real-time Control Centers would need to adopt a common solution in order to minimize complexity and cost.

Likes 2	Hydro One Networks, Inc., 1, Farahbakhsh Payam; Hydro One Networks, Inc., 3, Malozewski Paul
Dislikes 0	

Response

Dermot Smyth - Con Ed - Consolidated Edison Co. of New York - 5, Group Name Con Edison

Answer	
Document Name	

Comment

CIP-012-1 should be aligned with TOP-003-3. Data security is already required in TOP-003-3 R5. Only data that is stipulated in the TOP-003-3 R1 data specification for Operational Planning Analysis, Real-time Assessment, and Real-time monitoring should be in scope for CIP-012.

The proposed standard does not make clear how entities should work together when addressing security concerns across a communication network link. Some guidance regarding joint handling of communication links would be helpful. Where does the obligation for protecting a link per entity start and end?

Likes 0	
Dislikes 0	

Response

Brandon McCormick - Brandon McCormick On Behalf of: Ginny Beigel, City of Vero Beach, 3; Lynne Mila, City of Clewiston, 4; Tom Reedy, Florida Municipal Power Pool, 6; - Brandon McCormick, Group Name FMPA

Answer	
Document Name	

Comment

FMPA believes that the proposed standard does not make clear how entities should work together when addressing security concerns across a communication network link. Some support for joint handling of issues should be made clear.

FMPA believes that an Implementation Guidance document should be developed and include guidance on possible determination of the security method used being developed at the regional or RC level. This may facilitate a more cost-effective approach. Moreover, the Implementation Guidance could also address the entities evidence needed when they are following what was determined by the Region, RC or ISO.

Likes 0	

Dislikes 0	

Response

David Rivera - New York Power Authority - 3	
Answer	
Document Name	

Comment
The proposed standard does not make clear how entities should work together when addressing security concerns across a communication network link. Some support for joint handling of issues could be made clear. Where does the obligation for protecting a link per entity start and end? Note: These comments are equivalent to those submitted by the NPCC/TFIST group, except for changes in the Yes/No answers.

Likes 0	
Dislikes 0	

Response

Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	
Document Name	

Comment
1. The NSRF questions the use of “Real-time monitoring” as an applicable object within R1. “Real-time” is defined as “present time as opposed to future time”. Which our industry understands and without the word “monitoring” being defined, may lead to misinterpretation by responsible entities and CEAs, alike. The word “monitoring” may mean ALL monitoring of an entity’s entire SCADA system. It should be the “monitoring” of BES data, only, that is required for Operational Planning Analysis and Real-time Assessments. 2. The Applicability section states, “For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly”. This proposed Standard does not specify any specific entities and we recommend that this is removed. 3. The NSRF has concerns with the proposed definition of Control Center. The largest issue is the last paragraph concerning a Generating Operator. The use of the word “capability” is ambiguous and will confuse Registered Entities and CEAs, a like. The SDT should consider the approved Applicability within PER-005-2 part 4.1.5.1, which reads: *Dispatch personnel at a centrally located dispatch center who receive direction from the Generator Operator’s Reliability Coordinator, Balancing Authority, Transmission Operator, or Transmission Owner, and may develop specific dispatch instructions for plant operators under their control. This personnel does not include plant operators located at a generator plant site or personnel at a centrally located dispatch center who relay dispatch instructions without making any modifications.* This aligns with current and understood wording of PER-005-2.

4. Are the noted “Real-time reliability related- tasks” within the proposed definition, the same “Real-time Reliability-related task prescribed in PER-005-2? If so, please state this in your consideration of comments document and within your guidance document.

5. The NSRF believes that data associated with Operational Planning Analyses (OPA), Real-time monitoring (RTm), and Real-time Assessments (RTA) are predicated on other Standards and protection of data is required but all three areas (OPA, RTm, and RTA) are not subject equally to the Applicable Entities noted in CIP-012-1. Per IRO-010-2, R1, the RC is to document its specifications necessary for OPA, RTm, and RTA. Per TOP-003-3, R1 the TOP is to document its specifications necessary for OPA, RTm, and RTA. Per TOP-003-3, R2, the BA is to document its specifications necessary for analysis functions and RTm, only. The SDT, in the Technical Rationale and Justification document, acknowledges TOP-003 and IRO-010 “provides consistent scoping of identified data” [R1 section: Alignment with IRO and TOP Standards”]. The SDT should quantify that the data to be protected is the data associated with the Applicable entities with IRO-010-2 and TOP-003-3. With doing this, the SDT will articulate what the entity is to perform what analysis and what “data” is to be protected, based on already approved NERC Reliability Standards. By clearly identifying (and linking) the data to be protected from the data specifications developed under Standards TOP-003 and IRO-010, there is no room for interpretation of what “data” is to be protected.

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	
Document Name	

Comment

Although the FERC order specifies data between Control Centers, Texas RE notes that there is OPA, RTA, Real-time monitoring data that is not between control centers. For example, Distribution Providers provide BES sensitive data but would not be subject the standard. Also there are numerous GOPs that do not have a control center per the definition that provide BES sensitive data which also would not subject to CIP-012-1. Texas RE is concerned this creates a reliability gap since these scenarios would not be covered under the proposed draft of CIP-012-1.

Although Texas RE does not oppose a CIP Exceptional Circumstances exception from the implementation requirements set forth in CIP-012-1 R2, Texas RE requests that the SDT provide a rationale for why such an exception is appropriate. In particular, it is unclear why certain CIP exception conditions, such as an imminent hardware failure, should necessarily trigger a relaxation of physical security protections for communications links transmitted sensitive data in all circumstances.

Likes 0	
Dislikes 0	

Response

Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body

Answer	
Document Name	

Comment	
See APPA Comments.	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1	
Answer	
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Marty Hostler - Northern California Power Agency - 5	
Answer	
Document Name	
Comment	
Refer to APPA, TAPs, and Utility Services comments.	
Likes 0	
Dislikes 0	
Response	
Dennis Sismaet - Northern California Power Agency - 6	
Answer	
Document Name	
Comment	

Refer to APPA, TAPs, and Utility Services comments.

Likes 0	
Dislikes 0	

Response

Vivian Vo - APS - Arizona Public Service Co. - 3

Answer	
Document Name	

Comment

AZPS reiterates its comments provided in response to Requirement R1 regarding clear delineation of responsibilities between receiving and transmitting entities. Because the potential impacts of a receiving entity not appropriately implementing the technology needed for decryption or use of protected data sent by a transmitting entity lie outside of the proposed Requirement R1 in real-time data and assessment obligations, placement of the obligations for Requirement R1 on the transmitting is appropriate and reduces the potential for double jeopardy and/or “waterfall” non-compliance events. Hence, AZPS suggests that it is appropriate to place the obligation for Requirement R1 on the transmitting entity.

Finally, AZPS reiterates the NERC ORD as a reference guide and resource regarding the scope of this standard and sensitive data generally. The NERC ORD Agreement has long maintained an accepted, well-established definition for sensitive reliability data. That definition does not include data utilized in the Operational Planning Horizon and, for the reasons discussed above, AZPS asserts that the inclusion of Operational Planning Analysis in Requirement R1 extends the scope of BES sensitive data without attendant benefit to reliability. AZPS recommends the deletion of Operational Planning Analysis from Requirement R1 to allow the Requirement to remain consistent with well-established, well understood precedent as set forth in the NERC ORD Agreement.

Likes 0	
Dislikes 0	

Response

Quintin Lee - Eversource Energy - 1, Group Name Eversource Group

Answer	
Document Name	

Comment

Clarification needed – Does 'data used for Operational Planning Analysis, Real-time Assessments, and Real-time monitoring ' include Generator Unit Commitment Data and/or transmission and generator outages which are posted publicly?

Likes 0	
Dislikes 0	

Response	
Aaron Austin - AEP - 3	
Answer	
Document Name	CIP-012-1 – Cyber Security -Communication Networks Diagram.doc
Comment	
AEP suggests these should be added to the diagram as clearly in scope.	
Likes 0	
Dislikes 0	
Response	
Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	
Document Name	
Comment	
NRECA appreciates the continuing efforts of the SDT.	
Likes 0	
Dislikes 0	
Response	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	
Document Name	
Comment	
The proposed standard does not make clear how entities should work together when addressing security concerns across a communication network link. Some support for joint handling of issues could be made clear. Where does the obligation for protecting a link per entity start and end?	

Likes 0	
Dislikes 0	

Response

Lona Calderon - Salt River Project - 1,3,5,6 - WECC

Answer	
Document Name	

Comment

One challenge associated with CIP-012-1 is industry-wide coordination would be necessary to successfully implement encryption.

In addition to adding latency, encryption adds burden for ongoing maintenance and management for an encryption program. SRP agrees with LPPC that guidance is needed on key management and inter utility agreements pertaining to coordination for encryption of data and impacts on real-time operation of the Bulk Electric System.

Likes 0	
Dislikes 0	

Response

Thomas Breene - WEC Energy Group, Inc. - 3

Answer	
Document Name	

Comment

1. We question the use of “Real-time monitoring” as an applicable object within R1. “Real-time” is defined as “present time as opposed to future time”. Which our industry understands and without the word “monitoring” being defined, may lead to misinterpretation by responsible entities and CEAs, alike. The word “monitoring” may mean ALL monitoring of an entity’s entire SCADA system. It should be the “monitoring” of BES data, only, that is required for Operational Planning Analysis and Real-time Assessments.

2. The Applicability section states, “For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly”. This proposed Standard does not specify any specific entities and recommend that this be removed.

3. We have concerns with the proposed definition of Control Center. The largest issue is the last paragraph concerning a Generating Operator. The use of the word “capability” is ambiguous and will confuse Registered Entities and CEAs, a like. The SDT should consider the approved Applicability within PER-005-2 part 4.1.5.1, which reads:

Dispatch personnel at a centrally located dispatch center who receive direction from the Generator Operator's Reliability Coordinator, Balancing Authority, Transmission Operator, or Transmission Owner, and may develop specific dispatch instructions for plant operators under their control. These personnel do not include plant operators located at a generator plant site or personnel at a centrally located dispatch center who relay dispatch instructions without making any modifications.

This aligns with current and understood wording of PER-005-2.

4. Are the noted "Real-time reliability related- tasks" within the proposed definition, the same "Real-time Reliability-related task prescribed in PER-005-2? If so, please state this in your consideration of comments document and within your guidance document.

5. We believe that data associated with Operational Planning Analyses (OPA), Real-time monitoring (RTm), and Real-time Assessments (RTA) are predicated on other Standards and protection of data is required but all three areas (OPA, RTm, and RTA) are not subject equally to the Applicable Entities noted in CIP-012-1. Per IRO-010-2, R1, the RC is to document its specifications necessary for OPA, RTm, and RTA. Per TOP-003-3, R1 the TOP is to document its specifications necessary for OPA, RTm, and RTA. Per TOP-003-3, R2, the BA is to document its specifications necessary for analysis functions and RTm, only. The SDT, in the Technical Rationale and Justification document acknowledges TOP-003 and IRO-010 "provides consistent scoping of identified data" [R1 section: Alignment with IRO and TOP Standards"]. The SDT should quantify that the data to be protected is the data associated with the Applicable entities with IRO-010-2 and TOP-003-3. With doing this, the SDT will articulate what the entity is to preform what analysis and what "data" is to be protected, based on already approved NERC Reliability Standards. By clearly identifying (and linking) the data to be protected from the data specifications developed under Standards TOP-003 and IRO-010, there is no room for interpretation of what "data" is to be protected.

Likes 0	
Dislikes 0	

Response

Russell Noble - Cowlitz County PUD - 3

Answer	
Document Name	

Comment

Although Cowlitz PUD agrees with the intent of the proposed standard, we are concerned the protective measures developed by entities could have unintended consequences. In particular, there is concern encryption could unacceptably slow data transmission.

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Con-Edison and Dominion

Answer	
Document Name	
Comment	

· The proposed standard does not make clear how entities should work together when addressing security concerns across a communication network link. Some support for joint handling of issues could be made clear. Where does the obligation for protecting a link per entity start and end?

Likes 0	
Dislikes 0	
Response	

Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2

Answer	
Document Name	
Comment	

ERCOT ISO signs on to the ITC SWG comments:

The ITC SWG asserts that the proposed standard does not make clear how entities should work together when addressing security concerns across a communication network link. If both entities work with CIP Standard assumptions on both ends of a communication network, some support for joint handling of issues could be made clear. However, if only one entity is CIP-compliant for a given link, the current standard draft does not make clear the extent of protection expected for the data. The Standard should provide more information on the ownership of obligations for protecting the entire link.

It is unclear whether the addition of CIP-012 affects the exemptions of communication networks in any of the applicability sections of other standards (CIP-002 through CIP-011). The SWG requests clarification that CIP-012 fills in some of the gap created the CIP-002 – CIP-011 third party telecommunications exemption (4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.)

It has been ten years since the SANDIA report (“Secure ICCP Considerations and Recommendations”), the only detailed report on this subject which could be considered close having entered mainstream awareness in the industry. Today, as ten years ago, Secure ICCP is not a viable choice for utilities, if only due to limited community experience and vendor support, not to mention the complexities of key management. The transition strategies that SANDIA discusses – Layer 3 protection using IPsec and Layer 2 protection with hardware encryption – remain today’s target solutions.

WECC, and specifically the WECC DEMSWG (Data Exchange and EMS Working Group) has been working with Pacific Northwest National Laboratory (PNNL) for some time on a new evaluation of Secure ICCP. PNNL recently completed their work and presented the results to DEMSWG in 2016. The PNNL study functionally succeeded but with enough limitations that PNNL was prompted to conclude that it would be difficult to make a business case for implementing Secure ICCP when other solutions are available.

IPsec is a viable alternative. Over MPLS, IPsec could secure GRE tunnels between CE routers. Challenges with this approach include the possibility of having to hire a third party to manage certificates and IPsec links, especially for ISOs that do not manage their own MPLS networks.

The ITC SWG position on security architecture is that business transactions (such as ICCP) should not be tightly coupled with encryption technologies. Solutions should prefer network overlays versus security extensions to a protocol (such as Secure ICCP or DNP3 SA).

The security architecture should prefer least-latent encryption solutions at the Ethernet or IP layers of the network stack. MACsec (802.1AE) models the spirit of an optimal solution within a metro area – could it scale wider?

The ITC SWG's overall position on Secure ICCP is that it represents too much reliability risk. The ITC SWG is concerned about the lack of open standards and protocols available to meet the confidentiality and integrity security objectives of CIP-012. Assuming that a solution involves encryption, the only two open standards and protocols that can meet the CIP-012 security objectives are IPsec and TLS. The potential for vendor leverage in such a small open solution space is large. Vendor-managed MPLS networks, typical among utilities, already entrench high annual telecommunication costs in utility budgets. Security vendors continue to benefit from the expense of establishing layered cyber defenses. Open Source solutions provide a cost and agility refuge from this lopsided value chain without compromising defense layers. The trend toward managed services makes the cost problem worse for utilities, especially in the context of insufficiently evaluated risk. Vendor leverage only grows given the practical consideration that all the communicating parties in a WAN of connected real-time Control Centers would need to adopt a common solution in order to minimize complexity and cost.

Likes 0	
Dislikes 0	

Response

Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 3

Answer	
Document Name	

Comment

Tacoma Power supports the comments of APPA

Likes 0	
Dislikes 0	

Response

Theresa Rakowsky - Puget Sound Energy, Inc. - 1

Answer	
Document Name	

Comment

n/a

Likes 0	
Dislikes 0	

Response

Jack Cashin - American Public Power Association - 4	
Answer	
Document Name	
Comment	
APPA believes that the proposed standard does not make clear how entities should work together when addressing security concerns across a communication network link. Some support for joint handling of issues should be made clear. Public power believes that an Implementation Guidance document should be developed and include guidance on possible determination of the security method used being developed at the regional or RC level. This may facilitate a more cost-effective approach. Moreover, the Implementation Guidance could also address the entities evidence needed when they are following what was determined by the Region, RC or ISO.	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	
Document Name	
Comment	
The STD should consider changing the title of the CIP-012-1 requirement to “CIP-012-1-Cyber Security – Control Center Communication **Links**” to align with the language in FERC Order No. 822 and the language in Requirement R1. The current use of the term “Networks” may be misleading because it implies a broader scope of communication. Additionally, the violation severity levels (VSL) for this requirement is limited to “Severe”. CenterPoint Energy recommends that Requirement R1 VSL be “Moderate” to “High” due to the fact that Requirement R1 is a documentation requirement.	
Likes 0	
Dislikes 0	
Response	
David Greene - SERC Reliability Corporation - 10, Group Name SERC CIPC	
Answer	
Document Name	
Comment	

NA	
Likes 0	
Dislikes 0	
Response	
Warren Cross - ACES Power Marketing - 1,3,4,5 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standards Collaborators	
Answer	
Document Name	
Comment	
We thank you for this opportunity to provide these comments.	
Likes 0	
Dislikes 0	
Response	
Sheranee Nedd - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	
Document Name	
Comment	
PSEG supports the NPCC comments.	
Likes 1	PSEG - PSEG Fossil LLC, 5, Kucey Tim
Dislikes 0	
Response	
Michael Puscas - ISO New England, Inc. - 2	
Answer	
Document Name	
Comment	
Comments:	

- The proposed standard does not make clear how entities should work together when addressing security concerns across a communication network link. If both entities work with CIP Standard assumptions on both ends of a communication network, some support for joint handling of issues could be made clear. However, if only one entity is CIP-compliant for a given link, the current standard draft does not make clear the extent of protection expected for the data. Where does the obligation for protecting a link per entity start and end?

- Does the addition of CIP-012 affect the exemptions of communication networks in any of the applicability sections of other standards (CIP-002 through CIP-011)?

- While the CIP standards should emphasize outcomes and allow entities to achieve specific security objectives in many ways, protections applied to communications should be evaluated with due consideration of the context in which people, processes and technology are applied to establish a given security protection. Demonstration of risk mitigation should include assessment of not just technology and process to provide protection, but also the diversity and severity of threats present in a given context (e.g. the difference between dedicated communication links as opposed to broadly shared communications infrastructure). Particular technology and process applied in a context with fewer or lower likelihood threats should be preferred over the same technology and process in a context with more or greater likelihood threats (i.e. greater overall risk). Simply specifying that some (how much?) risk mitigation should be applied by means that include physical, logical and possibly other means leads to insufficient conditions for establishing compliance both for the responsible entity and anyone reviewing compliance for that entity. Entities should consider not only that risk mitigation should take place, but also the thresholds for residual risk that should be considered acceptable for such communication.

- It should be noted that in a recent report from the National Infrastructure Advisory Council (NIAC) to the DHS and President of the United States, the NIAC recommended that separate communication networks be used for critical communications (reference https://www.dhs.gov/publication/niac-securing-cyber-assets-addressing-urgent-cyber-threats-critical-infrastructure-final, report page 3, first recommendation).

Likes 0	
Dislikes 0	

Response

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	
Document Name	

Comment

BPA suggests adding the verbiage “where technically feasible” to the requirements, in order to implement controls where appropriate, based on the technology (as discussed in Q1) and risk.

Likes 0	
Dislikes 0	

Response

Brian Evans-Mongeon - Utility Services, Inc. - 4

Answer	
Document Name	

Comment
Utility Services believes that the proposed standard does not make clear how entities should work together when addressing security concerns across a communication network link. Some support for joint handling of issues should be made clear. Utility Services believes that an Implementation Guidance document should be developed and include guidance on possible determination of the security method used being developed at the regional or RC level. This may facilitate a more cost-effective approach. Moreover, the Implementation Guidance could also address the entities evidence needed when they are following what was determined by the Region, RC or ISO.

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	

Comment
If the SDT retains a data-centric approach, we believe the time element is very important and is correctly captured in the requirement with the phrase “while being transmitted between Control Centers.” We encourage the SDT to retain this language. We note the RSAW drops the time element and just says “transmitted between”. The time element is very important, as data transmitted between Control Centers a year ago is not the focus of this standard. This will, ideally, be reflected in the Standard itself, as well as the Technical Rationale and the RSAW, for clarity.

Likes 0	
Dislikes 0	

Response

David Ramkalawan - Ontario Power Generation Inc. - 5

Answer	
Document Name	

Comment
OPG understands the focus is on protection of data communication between control centers but would like to clarify that it is not being required to verify integrity of data from it’s origination points to the point where it’s first aggregated at a control center, as this would be a substantially more difficult and costly requirement to achieve.

Likes 0	
Dislikes 0	

Response

Ronald Donahey - TECO - Tampa Electric Co. - 3

Answer	
Document Name	

Comment

Tampa Electric appreciates the efforts of the Standards Drafting Team in developing protections for Communication Networks. We have concerns that the scope of the standard regarding data protection (based on IRO-010 and TOP-003) extends the requirement to data/information that is not currently required to be protected at the level of a High Impact BES Cyber System. This approach does not match the intent and protections of all other NERC CIP standards.

Likes 0	
Dislikes 0	

Response

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group

Answer	
Document Name	

Comment

The SPP Standards Review Group recommends the drafting team verifies and confirms that the NERC defined terms ‘Operational Planning Analyses’, ‘Real-time Assessments’, and ‘Real-time’ (mentioned in the Rationale Section in reference to Requirement R1) are defined and properly aligned with the Rules of Procedure (RoP) documentation. We have a concern that if the terms aren’t properly defined and aligned in both documents that this could lead to potential interpretation issues for future projects. During the verification process, should the drafting team discover that there is supporting evidence to SPP’s concerns, we would recommend the drafting team developing a Standard Authorization Request (SAR) to help ensures that both documents have consistency in the definition of the terms mentioned.

The SPP Standard Review Group would ask the drafting team to provide clarity on why the RoP is not mentioned in the Implementation Plan like the NERC Glossary of Terms. From our perspective, the RoP and the definitions, it contains have the same significance that the Glossary of Terms have in reference to the industry defined terms.

Likes 0	
Dislikes 0	

Response

Wendy Center - U.S. Bureau of Reclamation - 5	
Answer	
Document Name	
Comment	
Reclamation recommends the SDT define the term “Real-time monitoring” in the NERC Glossary of Terms. The Applicability section states, “For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.” No Requirements in this proposed Standard explicitly specify a functional entity or entities; therefore, Reclamation also recommends that this sentence be removed.	
Likes 0	
Dislikes 0	
Response	

Scott Berry - Scott Berry On Behalf of: Jack Alvey, Indiana Municipal Power Agency, 1, 4; - Scott Berry	
Answer	
Document Name	2016-02_Unofficial_Comment_Form_Control_Center_Definition_08142017.docx
Comment	
IMPA is attaching its comments for Control Center. The feedback/survey sheet is not linked to this vote. Our Control Center survey response is attached.	
Likes 0	
Dislikes 0	
Response	

Lauren Price - American Transmission Company, LLC - 1	
Answer	
Document Name	
Comment	
Not Applicable	
Likes 0	
Dislikes 0	

Response
Laura McLeod - NB Power Corporation - 5
Answer	
Document Name	
Comment
No additional comments.
Likes 0	
Dislikes 0	
Response
Haley Sousa - Public Utility District No. 1 of Chelan County - 5
Answer	
Document Name	
Comment
Implementing industry-wide secure communication is a significant coordination challenge for entities and their associated vendors. The increase in security also brings increased complexity, maintenance, and failure potential that may negatively impact the reliable operation of the BES. As a result, coordination for encryption key management will become an essential activity and CHPD would, similar to other entity comments, appreciate guidance for these activities.
Likes 0	
Dislikes 0	
Response
Douglas Webb - Douglas Webb On Behalf of: Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 3, 5, 1, 6; James McBee, Great Plains Energy - Kansas City Power and Light Co., 3, 5, 1, 6; Jessica Tucker, Great Plains Energy - Kansas City Power and Light Co., 3, 5, 1, 6; Jim Flucke, Great Plains Energy - Kansas City Power and Light Co., 3, 5, 1, 6; - Douglas Webb
Answer	
Document Name	
Comment
None.
Likes 0	

Dislikes 0	
Response	
Janis Weddle - Public Utility District No. 1 of Chelan County - 6	
Answer	
Document Name	
Comment	
Implementing industry-wide secure communication is a significant coordination challenge for entities and their associated vendors. The increase in security also brings increased complexity, maintenance, and failure potential that may negatively impact the reliable operation of the BES. As a result, coordination for encryption key management will become an essential activity and CHPD would, similar to other entity comments, appreciate guidance for these activities.	
Likes 0	
Dislikes 0	
Response	

Comments from David Greene, SERC

Questions

1. Requirement R1: The SDT drafted CIP-012-1 Requirement R1 to meet the mandatory requirement for the Responsible Entity to develop one or more documented plan(s) to mitigate the risk of the unauthorized disclosure or modification of data used for Operational Planning Analysis, Real-time Assessment, and Real-time monitoring data while being transmitted between Control Centers. Do you agree with this revision? If not, please provide the basis for your disagreement and an alternate proposal.

   ☐ Yes
   ☒ No
   Comments:

   - **Revise R1.** First paragraph, remove "Operational Planning Analysis"

     Rationale: Operational Planning Analysis data does not impact the BES within 15 minutes. The systems handling Operational Planning Analysis data are typically separate from the systems performing real-time BES analysis/control.

     The data involved with Operational Planning is "theoretical", e.g., requests to take a line out of service or de-rate a generation unit. If an event occurs in real-time to trip a line or de-rate a unit, information is immediately conveyed via a mechanism other than Operational Planning data.

Because the Operational Planning data is requesting permission to do something, the request will be validated by other measures – e.g., permission to take the line out of service/de-rate the unit, followed (later) by switching orders to take the line out of service or revised bid into the generation market indicating the unit will only provide the de-rated output.

Thus, because it does not directly impact the reliable operation of the BES and cross-checks are already built into the data process, stringent controls for data transfer is not required.

2. Requirement R1: The SDT seeks comment on the need to scope sensitive BES data as it applies to Operational Planning Analysis, Real-time Assessment, and Real-time monitoring. Do you agree with scoping CIP-012-1 Requirement R1 in this manner? Please provide comment in support of your response.

☐ Yes
☒ No
Comments:

- **Revise R1.** First paragraph, remove "Operational Planning Analysis"

  Rationale: Operational Planning Analysis data does not impact the BES within 15 minutes. The systems handling Operational Planning Analysis data are typically separate from the systems performing real-time BES analysis/control.

  The data involved with Operational Planning is "theoretical", e.g., requests to take a line out of service or de-rate a generation unit. If an event occurs in real-time to trip a line or de-rate a unit, information is immediately conveyed via a mechanism other than Operational Planning data.

  Because the Operational Planning data is requesting permission to do something, the request will be validated by other measures – e.g., permission to take the line out of service/de-rate the unit, followed (later) by switching orders to take the line out of service or revised bid into the generation market indicating the unit will only provide the de-rated output.

  Thus, because it does not directly impact the reliable operation of the BES and cross-checks are already built into the data process, stringent controls for data transfer is not required.

3. Implementation Plan: The SDT revised the Implementation Plan such that the standard and NERC Glossary terms are effective the first day of the first calendar quarter that is twelve (12) calendar months after the effective date of the applicable governmental authority's order approving the standard, or as otherwise provided for by the applicable governmental authority. Do you agree with this proposal? If you agree with the proposed implementation time period, please note the actions you will take that require this amount of time to complete. If you think an alternate implementation time period is needed – shorter or longer - please propose an alternate implementation plan and provide a detailed explanation of actions and time needed to meet the implementation deadline.

☐ Yes

☒ No
Comments:

- **Alternate Implementation Period**: 2 Year Implementation Plan Period

  Rationale: There are a number of factors to consider, and all affect the time required to implement, to include the following:
  - Complexity of the technology solutions to be implemented,
  - Number of interconnecting lines to secure,
  - Troubleshooting/testing at each connection point, and
  - Coordination requirements with external stakeholders

4. The SDT believes proposed CIP-012-1 provides entities with flexibility to meet the reliability objectives in a cost effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost effective approaches, please provide your recommendation and, if appropriate, technical justification.

   ☒ Yes
   ☐ No
   Comments:

5. If you have additional comments on the proposed CIP-012-1 – Cyber Security -- Communication Networks drafted in response to the FERC directive that you have **not** provided in response to the questions above, please provide them here.

   Comments: NA

Comments from Vivian Vo, APS

Questions

1. Requirement R1: The SDT drafted CIP-012-1 Requirement R1 to meet the mandatory requirement for the Responsible Entity to develop one or more documented plan(s) to mitigate the risk of the unauthorized disclosure or modification of data used for Operational Planning Analysis, Real-time Assessment, and Real-time monitoring data while being transmitted between Control Centers. Do you agree with this revision? If not, please provide the basis for your disagreement and an alternate proposal.

   ☒ Yes
   ☐ No

   Comments:

   AZPS respectfully submits that, as written, the allocation of responsibilities between transmitting and receiving entities is unclear. Delineation of these responsibilities is essential because a receiving entity has no control over the behavior, implementation, and/or lack of

implementation of third-party entities and cannot prevent third-party entities from transmitting unprotected data. As written, Requirement R1 could be construed as holding both the transmitting and receiving entity responsible where the transmitting entity fails to implement its plan. The receiving entity would only be aware/in receipt of the protected or unprotected data once it is transmitted by the transmitting entity. At which point, the potential for non-compliance has already occurred. Accordingly, because the data emanates from the transmitting entity, the data protection obligation should emanate from the transmitting entity.

For this reason, Requirement R1 should not hold receiving entities responsible for receiving data from another entity that failed to implement its plan. Responsibility for CIP-012-1 R1 should be placed clearly upon the transmitting entity and AZPS requests that the SDT modify Requirement R1 to ensure that there is a clear allocation of responsibilities between the transmitting and receiving entities. AZPS submits for consideration by the SDT a revised Requirement R1 below with language clarifying the allocation of responsibilities

> **R1.** The Responsible Entity shall develop one or more documented plan(s) to mitigate the risk of the unauthorized disclosure or modification of data used for Operational Planning Analysis, Real-time Assessments, and Real-time monitoring ~~while being transmitted~~ when transmitting data from one Control Center to another Control Center ~~between Control Centers~~. This excludes oral communications. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

The above proposed revisions clarify allocation of responsibilities without compromising on the level of required protection and while maintaining recognition that meaningful, logically protected communication that can be decrypted for use by the receiving entity requires bilateral agreement between the transmitting entity and receiving entity.

Comments from Scott Berry, Indiana Municipal Power Agency

Proposed Definition of "Control Center"

Revised Definition:
One or more facilities, including their associated data centers, that monitor and control the Bulk Electric System (BES) and host operating personnel who perform Real-time reliability-related tasks of: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for Transmission Facilities at two or more locations, or 4) a Generator Operator for generation Facilities at two or more locations.

For Reliability Coordinators, Balancing Authorities, and Transmission Operators, the operating personnel above are System Operators.

For Transmission Owners performing the Real-time reliability-related tasks of a Transmission Operator, the operating personnel above consist of personnel, excluding field switching personnel, who can act independently to operate or direct the operation of the Transmission Owner's Bulk Electric System Transmission Facilities in Real-time.

For Generator Operators, the operating personnel above consist of dispatch personnel at a centrally located dispatch center who receive direction from the Generator Operator's Reliability Coordinator, Balancing Authority, Transmission Operator, or Transmission Owner, and have the capability to develop specific dispatch instructions for plant operators under their control. These personnel do not include plant operators located at a generator plant site or personnel at a centrally located dispatch center who relay dispatch instructions without making any modifications.

Redline Definition:

One or more facilities, including their associated data centers, that monitor and control the Bulk Electric System (BES) and host ~~hosting~~ operating personnel ~~that monitor and control the Bulk Electric System (BES) in real-time to~~ who perform ~~the~~ Real-time reliability-related tasks~~, including their associated data centers,~~ of: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for Transmission Facilities at two or more locations, or 4) a Generator Operator for generation Facilities at two or more locations.

For Reliability Coordinators, Balancing Authorities, and Transmission Operators, the operating personnel above are System Operators.

For Transmission Owners performing the Real-time reliability-related tasks of a Transmission Operator, the operating personnel above consist of personnel, excluding field switching personnel, who can act independently to operate or direct the operation of the Transmission Owner's Bulk Electric System Transmission Facilities in Real-time.

For Generator Operators, the operating personnel above consist of dispatch personnel at a centrally located dispatch center who receive direction from the Generator Operator's Reliability Coordinator, Balancing Authority, Transmission Operator, or Transmission Owner, and have the capability to develop specific dispatch instructions for plant operators under their control. These personnel do not include plant operators located at a generator plant site or personnel at a centrally located dispatch center who relay dispatch instructions without making any modifications.

Currently Approved Definition:

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, of: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for transmission Facilities at two or more locations, or 4) a Generator Operator for generation Facilities at two or more locations.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Project 2016-02 Modifications to CIP Standards

Consideration of Comments for CIP-012-1

Initial Comment Period

October 27, 2017

RELIABILITY | ACCOUNTABILITY




Introduction

On January 21, 2016, the Federal Energy Regulatory Commission (FERC) issued Order No. 822 Revised Critical Infrastructure Protection Reliability Standards. In this order, FERC approved revisions to version 5 of the CIP standards. To address concerns identified in Order 822, FERC directed the development of modifications to the CIP Reliability Standards to require responsible entities to implement controls to protect, at a minimum, communication links and sensitive bulk electric system data communicated between bulk electric system Control Centers in a manner that is appropriately tailored to address the risks posed to the bulk electric system by the assets being protected (i.e., high, medium, or low impact).

The standard drafting team for Project 2016-02 developed an initial draft of proposed Reliability Standard CIP-012-1 to address the FERC directive and posted it for an initial 45-day comment period and ballot from July 27, 2017 through September 11, 2017. The SDT appreciates industry comments on the proposed Reliability Standard. The SDT considered the comments submitted during the initial posting of the proposed Reliability Standard, and revised the draft standard based on those comments. Additionally, the SDT conducted substantial outreach during the revision process, through in-person meetings, conference calls, and stakeholder organization presentations.

Summary Response to Comments

The SDT has carefully reviewed each stakeholder comment and has revised language where suggested changes are consistent with SDT intent and industry consensus. Also, several commenters suggested non-substantive language changes. The SDT has carefully considered each of these comments and has made revisions to further clarify the language. The SDT also made several changes to clarify the language and align it more closely with SDT intent and industry consensus. The SDT reviewed and responded to each comment in summary form below.

There were 81 sets of responses, including comments from approximately 207 different people from approximately 139 companies representing the 10 Industry Segments as shown in the table on the following pages. All comments submitted can be reviewed in their original format on the project page.

Our goal is to give every comment serious consideration in this process. If you feel that your comment has been overlooked, or was insufficiently addressed, please let us know by contacting the Senior Director, Standards and Education, Howard Gugel (via email) or at (404) 446-9693.

Question 1: CIP-012-1 Requirement R1

Summary Response

1. Requirement R1: The SDT drafted CIP-012-1 Requirement R1 to meet the mandatory requirement for the Responsible Entity to develop one or more documented plan(s) to mitigate the risk of the unauthorized disclosure or modification of data used for Operational Planning Analysis, Real-time Assessment, and Real-time monitoring data while being transmitted between Control Centers. Do you agree with this revision? If not, please provide the basis for your disagreement and an alternate proposal.

Move Note to Applicability Section

Several stakeholders expressed concerns about applicability type language in a note contained within Requirement 1 (R1). The Requirement R1 note provides: "If the Responsible Entity does not have a Control Center or it does not transmit the type of data specified in Requirement R1 of CIP-012-1 between two Control Centers, the requirements in CIP-012-1 would not apply to that entity." Certain commenters stated that the note should be in the Applicability section and thereby eliminate the need for this to be discussed as part of the RSAW.

SDT Response: The SDT revised the proposed Reliability Standard to remove the note from Requirement R1 and included the following in the Applicability section for Functional Entities: "that own or operate a Control Center."

Demarcation Point

Several commenters expressed that in order to evaluate the extent and kind of obligation involved with Requirement R1, the phrase "transmitted between two control centers," needs to be clarified. Clarification should include identification of the demarcation points of the link being protected.

One commenter noted that in many cases some types of operational planning analysis data is housed in systems not classified as BES Cyber Systems and may not reside within an ESP. The commenter stated that a documented plan provides a mechanism to identify and document flows of BES sensitive data that do not originate from within an ESP nor pass through an EAP.

At least one commenter expressed concerns with potential issues arising from communication links not owned by a Responsible Entity, as well as with the determination of demarcation points when the communication is performed between Control Centers belonging to different Responsible Entities.

More than one commenter noted that to evaluate the extent and kind of obligation involved, the definition of 'between control centers' needs to be clearer where pertaining to communication

links. They also commented that the Reliability Standard should address the proper demarcation points to show implementation and compliance. The commenters further noted that to clearly define the obligation of Responsible Entities, the required plan should include identification of the demarcation points, and information on the explicit agreements required on each end of the physical communication link to arrange and identify the demarcation. As an example, the commenters noted that where there is disagreement on how protection should be applied between two or more Responsible Entities, there is no process to resolve those disagreements. They also asked how the identification of demarcation points should be resolved when a Responsible Entity (e.g., a Reliability Coordinator) is receiving information from a third-party provider that is aggregating and submitting data on behalf of one or more Responsible Entities (e.g., a Transmission Operator). The commenters further noted that it does not appear that the proposed Reliability Standard addresses connection to the third-party provider, since they are not a Responsible Entity or even registered with NERC. The commenters further assert that the same situation may be present for Responsible Entities that use an outsourced data center provider for data provided to regulatory agencies that are not subject to CIP Standards.

SDT Response: The SDT incorporated the concept of demarcation points into the proposed draft of CIP-012-1 to clarify where protection must begin and can terminate. The SDT also included provisions allowing the Responsible Entity to choose these points based on what works most effectively in the Responsible Entity's environment.

Email Communication Should Be Excluded

Some commenters requested the exclusion for oral communications be extended to electronic mail. At least one commenter noted the precise nature of Operator-to-Operator communications, pointing out that "Oral Communications" are excluded. However, EOP-008 (Emergency Operating) Plans often specify using cell/text/email while in mid-failover to the backup site. The commenter asked whether or not those types of communications are intended to be excluded.

SDT Response: The SDT contends that if sensitive bulk electric system data is being transmitted via email, then those emails should be protected in some manner. Confidentiality and integrity concerns for this data exist regardless of data transmission means.

Plan Approach

Several commenters noted that having a plan does not add to the reliability of protecting applicable data, suggesting that having a plan is an unwarranted layer of compliance. At least one commenter asserted that, if a "plan" approach is maintained in CIP-012-1, the SDT should clarify their understanding of that Plan. That commenter provided CIP-003-6 as an example.

At least one commenter indicated that the term "plan" is more analogous to the development of a project that has actions to achieve a result by specific date; similar to an implementation plan for a NERC Reliability Standard. The commenter suggested that if it was the intention of the

SDT to require a Responsible Entity to have a documented set of requirements to protect the sensitive BES data transmitted between the Control Centers then the term "policy" would be more appropriate. The commenter stated that a policy is interpreted to be more dynamic and ongoing throughout the lifetime of the requirement. The commenter adds that as cyber security technology is constantly changing and evolving, a policy would provide a definitive course of action for a Responsible Entity to protect sensitive BES data transmitted between the Control Centers.

SDT Response: The SDT contends that a plan will help a Responsible Entity ensure that all of the appropriate data is protected as required by draft CIP-012-1. Presenting this protection in an organized fashion, using a plan, will not only aid compliance efforts but will also help Responsible Entities ensure that the protection employed is optimal for their environments. The SDT notes that Responsible Entities can use a pre-existing plan or plans to satisfy CIP-012-1. This requirement structure is consistent with the language in the NERC Drafting Team Reference Manual.

Guidance Needed

More than one commenter requested that the SDT provide formal guidance for proposed Reliability Standard CIP-012-1. At least one commenter asserted that this is crucial for a Responsible Entity's understanding of how to meet the compliance objective of a new Reliability Standard.

One commenter noted that CIP-012-1 refers to data as outlined in NERC standards TOP-003-3 and IRO-010-2 that require protection. The commenter expressed the understanding that these types of data can vary based on Responsible Entity function and what data is needed. The commenter further notes that from a compliance monitoring perspective, it may be difficult to verify what the Responsible Entity is protecting versus what actually should be protected. The commenter requested that the SDT consider providing a list of typical data that should be protected per the standard and include it in guidance material. Another commenter noted that it is an overwhelming task to differentiate what are or are not confidential communications data over data links between Control Centers. Consequently, it is recommended that ALL data transmitted between Control Centers be protected. The standards should only address all data communication between control centers. Technologies such as encryption are generally implemented by link, not communication type.

More than one commenter requested that guidance language be provided for acceptable means of physically protecting communications links and identifying effective methods to mitigate risk.

SDT Response: The SDT appreciates all of the comments and suggestions, and will consider the appropriate mechanism by which to provide guidance for each of the issues identified.

Q1 Additional Comments

More than one commenter stated that the language in the proposed Reliability Standard should be in better alignment with the directives of the FERC order to establish a plan and implement controls to address the risks posed to the BES. At least one commenter noted that FERC emphasized that additional protection was required to protect both the "integrity and availability of sensitive bulk electric system data," FERC Order No. 822, P. 54. That commenter also noted that FERC made clear that this involved, at a minimum, two discrete actions: 1) that entities should implement controls to protect the physical communications links transmitting sensitive data between Control Centers; 2) that the sensitive data itself needed to be protected to ensure its accuracy and consistency. The commenter further stated that in issuing the directive subsequent to this rulemaking, FERC stated: "we adopt the NOPR proposal and direct that NERC . . . develop modifications to the CIP Reliability Standards to require responsible entities to implement controls to protect."

At least one commenter inquired as to why the FERC Order requires ". . . protect . . . data . . ." but the proposed R1 states to ". . . mitigate the risk of unauthorized disclosure or modification of data . . ."

SDT Response: The SDT asserts that the proposed CIP-012-1 Standard is in alignment with the directives in FERC Order No. 822 and has provided a Consideration of Issues and Directives document explaining its rationale. The SDT has established the security objective in Requirement R1 to address the Commission's directive on protecting the confidentiality (unauthorized disclosure) and integrity (unauthorized modification) of the data being transmitted.

At least one commenter expressed agreement with the creation of a new standard, rather than expanding CIP-003, CIP-005 and/or CIP-006 requirements to provide new controls over physical communication links.

SDT Response: The SDT thanks you for your support.

Another commenter requested that the SDT consider differentiating requirements for Control Center communications within a Responsible Entity from those for Control Center communications between different Responsible Entities. The commenter noted that data being sent for Reliability Standards TOP-003 and IRO-010 traverse the ICCP network maintained by a carrier, and Responsible Entities cannot provide physical protection for communication of this data from end to end. The commenter further stated that in the case of communications between different Responsible Entities, protecting the confidentiality and integrity can only be done through encryption. Since no single utility owns the hardware end to end on the ICCP network, site to site encryption cannot be implemented. The only options available would be application layer encryption or transport layer encryption utilizing IEC 62351-4 Secure ICCP. The commenter also noted that latency issues may occur from such data encryption.

SDT Response: The FERC Order specifically notes that the protection of sensitive BES data transmitted between Control Centers should be implemented for both inter- and intra-entity transmissions of data. The SDT intentionally did not restrict the language to Control Centers owned by a single Responsible Entity for this reason. Following the data specifications in the IRO and TOP standards would not be enough to fulfill this Order, unless appropriate controls are also included. The SDT cannot comment on specifics as to whether certain practices fulfill a Responsible Entity's compliance obligations.

More than one commenter noted that both TOP-003 and IRO-010 have a requirement that there be a mutually agreeable security protocol, and asked for the reason a new standard should be developed. The commenter further suggested the SDT consider modifying TOP-003 and IRO-010 if these standards do not provide adequate language to meet Order No. 822's concerns.

SDT Response: The SDT asserts that it is less confusing to keep all security-related requirements within the CIP family of standards. Also, the use of "mutually agreeable security protocol" does not encompass the intent of the Commission's Order, particularly around protecting the confidentiality and integrity of sensitive bulk electric system data. It is the position of the SDT that proposed CIP-012-1 and the TOP/IRO Requirements referred to in the comment complement one another.

At least one commenter suggested the addition of new requirement(s) to establish a hierarchy that requires Responsible Entities with the highest risk to set the communications security protocols. The commenter further suggested that Requirement R1 require Responsible Entities to have plans that follow the protocols set by the Responsible Entities higher in the hierarchical order.

SDT Response: It is the position of the SDT that it is appropriate to require the same protection for sensitive BES data while being transmitted between Control Centers, regardless of the impact level of the Control Center. The SDT has added a requirement part for coordination of responsibilities where multiple Responsible Entities are involved in the data transmission.

One commenter stated that proposed Reliability Standard CIP-012-1 is not necessary, and provided alternative proposals to address the risks by way of existing Reliability Standards such as CIP-003 and CIP-005.

SDT Response: The SDT determined that a new Reliability Standard is needed due to the interaction between all impact levels of BES Cyber Systems (i.e. high, medium, and low).

At least one commenter expressed disagreement with the use of two separate requirements, one for a plan and one to implement. That same commenter referred to CIP-004-011 as an example.

SDT Response: The SDT thanks you for your comment; however, the SDT elects to retain two

separate requirements.

One commenter pointed out that the Rationale discusses "CIP-012-1 Requirements R1 and R2 protection for applicable data during transmission between two geographically separate Control Centers;" The commenter asserted, however, that the requirements themselves don't seem to make that same distinction. The commenter stated that since the definition of a "Control Center" includes associated data centers, this could, for example, lead to the application of the proposed Reliability Standard to a facility that houses two control centers side-by-side (one with a data center downstairs). The commenter requested that the SDT provide more information about the rationale relative to geographical location and proximity of Control Centers, and corresponding language of the Requirements.

SDT Response: The SDT modified Requirement R1 to address data "transmitted between any Control Centers". This is irrespective of location and inclusive of the data centers as noted in the definition of Control Center.

One commenter noted that CIP-012-1 includes protection for data while being transmitted between Control Centers, and points out that Control Centers are facilities and do not transmit data. The commenter asked whether or not only data transmitted between BES Cyber Systems associated with a Control Center are included, or does it also include data transmitted by certified System Operators?

SDT Response: The SDT notes that data centers are included in the definition of Control Center. The data centers are traditionally the facilities that transmit the data. The data to be protected is Real-time Assessment and Real-time monitoring and control data transmitted between any Control Center.

At least one commenter stated that it is an overwhelming task to differentiate what is or what isn't confidential communications data over data links between Control Centers. The commenter recommended that all data transmitted between Control Centers be protected. The commenter further stated that technologies such as encryption are generally implemented by link, not communication type.

SDT Response: It is the position of the SDT that, in an establishing a plan for draft CIP-012-1, the Responsible Entity is not restricted to only protecting the data noted in the comment. If a Responsible Entity can achieve the security objective by protecting data on a larger scale, the Responsible Entity may do so.

One commenter noted that the Requirements should only permit the option to logically protect the data during transmission or at least remove the explicit options to physically protect the data, since physical protection is generally only available to address communication lines within the same facility. The commenter states that cryptography is the only mechanism available to protect

data across geographically dispersed Control Centers, and that presenting other options is confusing and has a strong potential to guide the industry toward ineffective solutions.

SDT Response: If an entity's environment is suited to use logical controls to protect the data as specified in CIP-012-1, they may do so. The same is the case if an entity's environment is suited for physical controls. This option is presented in case an entity decides, based on their environment, to use physical means in their protection scheme.

At least one commenter suggested that the SDT provide additional instruction within the Reliability Standard to address the requirements and implications for Balancing Authorities that serve as the Balancing Authority for other Responsible Entities. The commenter adds that it would be helpful to understand the Balancing Authority's responsibility to mitigate the risk of unauthorized disclosure or modification of data used for the analysis, assessment, and monitoring. The commenter also asked whether or not the Reliability Standard requirement for communications between control centers extends to communications between Responsible Entities and the Reliability Coordinators.

SDT Response: The SDT has drafted Requirement R1 to address data transmitted between Control Centers, including Reliability Coordinators, Balancing Authorities, and those they are interconnected with. The SDT has added a requirement part for coordination of responsibilities where multiple Responsible Entities are involved in the data transmission.

At least one commenter expressed concerns regarding the SDT addressing the CIP Version 5 Transition Advisory Group (V5TAG) identified issues with the CIP Version 5 Reliability Standard language that caused difficulty in implementation of the requirements. The commenter notes that the requirements, or another mechanism supplemental to CIP-005, needs to clarify the 4.2.3.2 exemption phrase "between discrete Electronic Security Perimeters."

SDT Response: The SDT thanks you for your comment. The SDT will be looking into addressing the v5TAG items noted in the near future. The SDT drafted CIP-012-1 without a dependency on an Electronic Security Perimeter for two reasons. First, the draft CIP-012-1 applies to Responsible Entities with high, medium, and/or low impact Control Centers. Since not all impact levels have defined Electronic Security Perimeters, CIP-012-1 is not based on them. Secondly, the Commission did not make note of Electronic Security Perimeters in Order 822, but rather that requirements are needed for Responsible Entities to protect sensitive BES data transmitted between Control Centers. The SDT will look into specifying demarcation points of where this protection would originate and terminate to clarify.

Question 2: CIP-012-1 Requirement R1 Scope

Summary Response

2. Requirement R1: The SDT seeks comment on the need to scope sensitive BES data as it applies

to Operational Planning Analysis, Real-time Assessment, and Real-time monitoring. Do you agree with scoping CIP-012-1 Requirement R1 in this manner? Please provide comment in support of your response.

Data used for Operational Planning Analysis should not be considered sensitive BES data.

Several commenters stated that data used for Operational Planning Analysis does not have a fifteen (15) minute impact on the reliability of the BES and should not be considered sensitive BES data. At least one commenter inquired if the 15-minute impact applicable to CIP-002 identification of BES Cyber Systems affects the applicability of CIP-012-1.

SDT Response: The SDT concluded that Operational Planning Analysis data, if rendered unavailable, degraded, or misused, would not adversely impact the reliable operation of the BES within 15 minutes of the activation or exercise of the compromise as detailed in CIP-002-5.1a. The SDT has revised the data in scope of proposed Reliability Standard CIP-012-1 to include only Real-time Assessment and Real-time monitoring and control data. The terms Real-time Assessments and Real-time used are defined in the Glossary of Terms Used in NERC Reliability Standards and used in TOP-003 and IRO-010, among other Reliability Standards.

Directly reference the data specification requirements in IRO-010 and TOP-003

At least one commenter stated that aligning proposed Reliability Standard CIP-012-1 with TOP-003-3 and IRO-010-2 is helpful for scoping CIP-012-1, and promotes consistent application of the NERC Standards.

Several commenters recommended proposed Reliability Standard CIP-012-1 include a direct reference to the data specification requirements in IRO-010 and TOP-003.

One commenter stated that the requirement as written does not meet the criteria as outlined in the document titled “Ten Benchmarks of an Excellent Reliability Standard.” The same commenter suggested that the SDT should draw a clear and unambiguous line to IRO-010 and TOP-003 within the CIP-012-1 requirement.

SDT Response: The SDT appreciates the comment but elects to use the defined terms from the Glossary of Terms used in NERC Reliability Standards to identify sensitive Bulk Electric System (BES) data, rather than directly referencing other Reliability Standards. The SDT discussed referencing the two applicable standards in the requirement language and determined that a number of issues could arise by directly referencing applicable IRO/TOP requirements. Possible issues include but are not limited to applicability issues and the required coordination of future revisions of the IRO/TOP standards and proposed Reliability Standard CIP-012-1.

Impact of encryption on system performance

More than one commenter noted that in addition to adding latency, encryption adds the burden of ongoing maintenance and management for an encryption program. The commenters also stated that guidance is needed on key management and inter utility agreements pertaining to coordination for encryption of data and impacts on real-time operation of the Bulk Electric System.

SDT Response: The SDT contends that the applicable data is not used for time sensitive protection or control functions, such as communications using protocol IEC TR-61850-90-5 R-GOOSE. The SDT asserts that technical solutions are available to address the security objective of the proposed requirement without hindering operational performance. The SDT intends to provide guidance for proposed Reliability Standard CIP-012-1. Additionally, should further guidance prove necessary, stakeholders may work with pre-certified entities to develop Implementation Guidance that may be submitted for ERO endorsement.

Data Type

One commenter asked whether or not "data used for Operational Planning Analysis, Real-time Assessments, and Real-time monitoring" includes Generator Unit Commitment Data and/or transmission and generator outages which are posted publicly.

More than one commenter stated that the requirement suggested data that are different from the data protected in other CIP standards, asserting that this may cause confusion in the future by calling it a CIP standard.

SDT Response: The SDT noted the reference in FERC Order No. 822 to additional Reliability Standards and the responsibilities to protect the data in accordance with those standards (TOP-003-3 and IRO-010-2). The SDT used these references to drive the identification of sensitive BES data and based proposed Reliability Standard CIP-012-1 on the data specifications in these standards. The SDT asserts that the data referenced by FERC Order No. 822 includes Real-time Assessment and Real-time monitoring and control data. The terms Real-time Assessments and Real-time used are defined in the Glossary of Terms Used in NERC Reliability Standards and used in TOP-003 and IRO-010, among other Reliability Standards. This data is inherently different than BES Cyber System Information. However, the security objective to protect the confidentiality and integrity of this data while being transmitted between Control Centers should reside in a Critical Infrastructure Protection Standard to be responsive to FERC Order No. 822.

Encrypt the link, not the data

Several commenters suggested that proposed Reliability Standard CIP-012-1 include language to require encrypting the link, not the data. The commenters note that technologies such as encryption or physical protection are generally implemented by link, not communication type.

Several commenters also suggested that further clarification on the scope of the data is needed to clarify that the data in question has already been scoped and is in specifications that are required by IRO-010 and TOP-003. The commenters also state that the SDT should consider doing away with a "data-centric" approach and focus protection on a more technical solution regardless of the type of data being transmitted between Control Center Electronic Security Perimeters and Low Impact Electronic Access Points.

SDT Response: The SDT has written the requirement to allow flexibility as to how to implement this requirement. This includes addressing the security objective without being prescriptive in the protections to be applied. The SDT noted the reference in FERC Order No. 822 to additional Reliability Standards and the responsibilities to protect the data in accordance with those standards (TOP-003 and IRO-010). The SDT used these references to drive the identification of sensitive BES data and based Reliability Standard CIP-012-1 on the data specifications in these standards. This approach provides consistent scoping of identified data, and does not require each entity to devise its own list or inventory of this data. Many Responsible Entities are required to provide this data under agreements executed with their Reliability Coordinator, Balancing Authority, or Transmission Operator, often without benefit of knowing how those entities use that data.

Add "BES" - to the R1 requirement language

At least one commenter noted that the FERC directive refers to "sensitive bulk electric system data" and directs NERC to "identify the scope of sensitive Bulk Electric System data," The commenter also states that the FERC directive also acknowledges that certain entities are already required to exchange necessary real-time and operational planning data through secured networks using mutually agreeable security protocol. At least one commenter requested the SDT consider scoping sensitive data explicitly to information exchanged between Control Centers' BES Cyber Systems. The commenters assert that the suggestion corresponds to the SDT's statement that "this data resides within BES Cyber Systems, and while at rest is protected by CIP-003 through CIP-011," and also corresponds to FERC's recognition of mutually agreeable security protocol networks referenced above. Also, at least one commenter stated that the entity needs to know what information is classified as BES sensitive data as it relates to operational planning analysis, real-time assessment, and real-time monitoring. The commenter notes that in many cases some types of operational planning analysis data is housed in systems not classified as BES Cyber Systems and may not reside within an Electronic Security Perimeter.

SDT Response: The SDT asserts that Real-time Assessment and Real-time monitoring and control data may not be limited to BES data. Please reference IRO-010-2, R1, Part 1.1, "1.1. A list of data and information needed by the Reliability Coordinator to support its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments <u>including non-BES data</u> and external network data, as deemed necessary by the Reliability Coordinator." The SDT further asserts that certain configurations exist where the demarcation point may not be a BES Cyber System. A scenario could exist where a router within a Physical Security Perimeter, but external to the Electronic Security Perimeter, encrypts the communication link between two

Control Centers. The router would not be categorized as a BES Cyber System, but the configuration would meet the security objective by implementing a combination of physical protection of the router and logical protection of the data.

Q2 Additional Comments

At least one commenter requested the SDT provide additional clarification on the protection of load forecasting data as it may not consistently be included as a separate BES Cyber System.

SDT Response: The SDT modified proposed Reliability Standard CIP-012-1, Requirement R1 to only apply to Real Time Assessment and Real Time monitoring and control data.

Question 3: Implementation Plan

Summary Response

3. Implementation Plan: The SDT revised the Implementation Plan such that the standard and NERC Glossary terms are effective the first day of the first calendar quarter that is twelve (12) calendar months after the effective date of the applicable governmental authority's order approving the standard, or as otherwise provided for by the applicable governmental authority. Do you agree with this proposal? If you agree with the proposed implementation time period, please note the actions you will take that require this amount of time to complete. If you think an alternate implementation time period is needed – shorter or longer - please propose an alternate implementation plan and provide a detailed explanation of actions and time needed to meet the implementation deadline.

Increase Implementation Time Period

Several commenters stated that additional time would be required to plan, budget, and implement proposed Reliability Standard CIP-012-1, and recommended Implementation time periods ranging from greater than twelve (12) months to 60 months.

More than one commenter noted that there are a number of factors to consider, and all affect the time required to implement. These factors include: 1) complexity of the technology solutions to be implemented; 2) number of interconnecting lines to secure; 3) troubleshooting/testing at each connection point; and 4) coordination requirements with external stakeholders, including coordination of plans across a large and/or diverse group of entities employing a variety of protective measures. At least one commenter cited the potential impact of having to redesign communications architectures for secure communications between Control Centers as rationale for extending the Implementation time period. Another commenter noted that smaller entities may need to procure equipment and implement technical controls that are not currently in place. The commenter further stated that the implementation of the plan(s) detailed in Requirement R1 could be impacted by budget cycles, procurement processes, and third party vendor

availability. At least one commenter suggested that modifications to the definition of Control Center may bring new Responsible Entities under the scope of CIP-012-1. The new Control Centers should be treated as "newly identified CIP facilities" and should be given an eighteen (18) month implementation period.

SDT Response: The SDT carefully considered all comments and concluded that many factors should be considered to determine an implementation period. These factors include complexity of technology solutions, quantity of telecommunications lines requiring controls and coordination with other Responsible Entities/solution providers. The SDT concluded that a twenty-four (24) month implementation period is appropriate.

Phased Implementation

Several commenters stated that proposed Reliability Standard CIP-012-1 will require a collaborative effort between Responsible Entities to achieve the required security for communications between Control Centers. They go on to state that it may not feasible for some Responsible Entities to implement the required security protection within 12 months. At least one commenter suggested that a phased approach may be more appropriate for proposed Reliability Standard CIP-012-1, based on schedules created using the Responsible Entity reliability hierarchy structure. As an example, at least one commenter noted that a Reliability Coordinator (RC) Control Center will have contact with the Control Centers of several Balancing Authorities (BA), Generator Operators (GOP), Transmission Operators (TOP), Transmission Owners (TO), and other RCs. If the first particular RC is unable to implement the protection required by NERC CIP-012-1 then there will be a cascading and unnecessary non-compliance effect among the other Responsible Entities interconnected with this particular RC's Control Center.

At least one commenter noted that applying protection between Control Centers owned by more than one Responsible Entity will involve significant coordination. Additional time would be necessary to develop a shared understanding of existing technical limitations, develop agreements, and implement those new approaches to achieve compliance. That same commenter indicated that additional time would allow the Responsible Entity to identify Control Centers that are in scope, decide on a method of protection, and involve any additional necessary parties.

One commenter noted the potential for replacement of equipment under existing contracts and requested that the affected contracts be exempted until new agreements can be put in place. A commenter further suggested that implementation of controls with telecommunications providers will require coordination and scheduling to align with the providers' resource availability and protect against any adverse impact on reliability. The commenter also suggests that renewal and renegotiation of existing contracts should not be required until they reach their expiration date.

SDT Response: The SDT carefully weighed a phased implementation plan for Requirement R1

and Requirement R2 of proposed Reliability Standard CIP-012-1. The SDT concluded, however, that such a plan with a monitored deadline for each of the requirements would add unnecessary complexity. Therefore, the SDT has concluded a twenty-four (24) month deadline would sufficiently meet the needs of industry.

Q3 Additional Comments

At least one commenter stated that Question 3 in the comment form implies there are NERC Glossary terms in the Implementation Plan, and states that there are no NERC Glossary terms in the proposed Implementation Plan for proposed Reliability Standard CIP-012-1.

SDT Response: The SDT agrees that there are not terms from the Glossary of Terms used in NERC Reliability Standards used in the proposed Implementation Plan for proposed Reliability Standard CIP-012-1.

One commenter requested that the SDT provide a specific justification for any proposed implementation timeframes, as well as for any revisions to the timeframes that are currently proposed. That same commenter requested that the SDT ensure there are no issues with the implementation plan, such as not having an initial performance date where one is needed, or not including information for new facilities, the commenter included an errata change in the PRC-023-4 implementation plan as an example.

SDT Response: The SDT has based the twenty-four (24) month implementation timeline on the comments received in the initial 45-day comment period and ballot from July 27, 2017 through September 11, 2017. Since there are no requirements that actions be performed on a defined frequency, there is no need to define an initial performance date.

Question 4: Cost Effectiveness

Summary Response

4. The SDT believes proposed CIP-012-1 provides entities with flexibility to meet the reliability objectives in a cost effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost effective approaches, please provide your recommendation and, if appropriate, technical justification.

Insufficient Information at this Time

Several commenters agreed that proposed Reliability Standard CIP-012-1 provides Responsible Entities with the flexibility to implement the standard cost-effectively and offered further suggestions to fully assess the logistics and costs associated with compliance. For example, some guidance or specification of boundaries for communications links involved would be required for entities to complete assessment of impacts to their operations.

Several commenters asserted that they cannot determine if the objectives may be accomplished in a cost-effective manner until further clarification is provided for physical or other equally effective protective measures and until the request for electronic mail exclusion is added. At least one commenter also noted concerns with vendor availability, regarding system software implementation that will be required for all entities industry-wide.

At least one commenter requested clarification that there is no requirement to verify integrity of data from its origin point to the point where it is first aggregated at a control center. The commenter states that this would make compliance with this requirement substantially more difficult and costly to achieve.

At least one commenter stated that for entities to fully assess the logistics, costs and operational impacts associated with compliance, some guidance or specification of boundaries of communications links involved would be required. One commenter stated that until industry is able to determine how much of the information requiring protection extends beyond the fifteen-minute time frame, the entity is not able to agree with the statement regarding cost-effective manner.

A commenter expressed concern that while the Standard is sufficiently flexible for an individual responsible entity, it leaves a potential gap between different Responsible Entities' interpretations of cost-effective approaches. The commenter noted that a large utility's view of cost effectiveness may not match a smaller neighbor's view of cost effectiveness. Such disparity could encumber agreement between the parties.

At least one commenter stated that the standard doesn't directly address the Inter-Control Center Communications Protocol (ICCP) for exchanging data between control centers or utilities. The commenter asked whether or not those ICCP servers and supportive infrastructure need to be upgraded or replaced with data encryption capabilities to support compliance with this standard.

One commenter stated that the standard doesn't provide any direction regarding the level of physical and logical protection that is mandatory. The commenter requested that the SDT develop guidance to clarify this ambiguity and identify how all entities can achieve a minimum level of compliance.

SDT Response: Thank you for your comments. The SDT recognizes that it is difficult to ascertain the level of cost effectiveness prior to implementation. The SDT has attempted to address cost effectiveness concerns by providing entities the latitude to determine the most appropriate implementation for their environment that meets the security objective rather than prescribing a specific approach to compliance. In cases where multiple entities are involved, the standard provides an obligation to identify the responsibilities of each of the organizations, but provides the organizations the latitude to determine the best approach for their environments so long

as the sensitive Bulk Electric System data is protected while being transmitted between Control Centers.

Cost Prohibitive

Several commenters asserted that there will likely be additional costs associated with administrative overhead, hardware, and software, as well as costs associated with monitoring the performance of the implemented solutions.

More than one commenter also noted that, Open Source options to satisfy the requirement to protect communication links and sensitive bulk electric system data communicated between Control Centers are limited. The commenters contend that fewer options generally translate to high vendor bargaining power, which could lead to high implementation costs. Those commenters also stated that it is unclear how or whether costs could be shared among participants in the network, and that architectural changes to support these requirements should be spread out over several years.

A commenter stated that security vendors continue to benefit from the expense of establishing layered cyber defenses, and that Open Source solutions provide a cost and agility refuge from this lopsided value chain without compromising defense layers. The commenter went on to state that the trend toward managed services makes the cost problem worse for utilities, especially in the context of insufficiently evaluated risk. The commenter further stated that vendor leverage only grows given the practical consideration that all the communicating parties in a WAN of connected real-time Control Centers would need to adopt a common solution in order to minimize complexity and cost.

SDT Response: Thank you for your comments. The SDT attempted to address cost effectiveness concerns by allowing entities the latitude to determine the most appropriate implementation for their environment that meets the security objective rather than prescribing a specific approach to compliance. The SDT is also proposing to lengthen the implementation plan to 24 months, which will allow entities additional time for any necessary changes to support these requirements.

Q4 Additional Comments

At least one commenter expressed agreement with the approach used in proposed Reliability Standard CIP-012-1 that allows each Registered Entity to analyze risk and use discretion in determining the best risk mitigation implementation for protecting transmission of applicable data.

SDT Response: Thank you for your support.

Question 5: Additional Comments

Summary Response

5. If you have additional comments on the proposed CIP-012-1 – Cyber Security -- Communication Networks drafted in response to the FERC directive that you have not provided in response to the questions above, please provide them here.

Many of the comments provided for Question 5 were provided and responded to in other questions.

Applicability

One commenter asked whether or not the Applicability section of proposed Reliability Standard CIP-012-1 may be modified to indicate that the standard only applies to those specific registered entities (e.g., GOPs and TOs) that maintain Control Centers AND transmit data between Control Centers.

One commenter stated that the Applicability section states, "For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly," while asserting that no Requirements in proposed Reliability Standard CIP-012-1 explicitly specify a functional entity or entities. That same commenter recommended the SDT remove the language quoted in the comment above.

A commenter stated that, pursuant to proposed Reliability Standard CIP-012-1, §4 Applicability, this standard is applicable to the Generator Owner, while noting that the proposed definition of Control Center exempts the Generator Owner as it only speaks to the Generator Operator's Control Center. The commenter further asserted that proposed Reliability Standard CIP-012-1 should not be applicable to the Generator Owner.

SDT Response: The SDT modified the applicability of the Standard as, "The requirements in this standard apply to the following functional entities, referred to as "Responsible Entities," that own or operate a Control Center." The SDT intends for the standard to include Generator Owners and Transmission Owners that own or operate a Control Center. The Control Center definition as written addresses the reliability tasks of an RC, BA, TOP, and GOP irrespective of registration. The SDT thanks you for the comments and is continuing to work on possible revisions to the definition to address these and other concerns.

CEC

At least one commenter questioned if using the phrase "CIP Exceptional Circumstances" is appropriately used in Requirement R2, since the intent is "to protect confidentiality and integrity of data transmitted between Control Centers required for reliable operation of the Bulk Electric

System (BES)." That same commenter asserts that CIP Exceptional Circumstances criteria are not relative to data transmission.

Another commenter requested that the SDT provide a rationale for including the phrase "CIP Exceptional Circumstances" in Requirement R2. That same commenter further stated that, in particular, it is unclear why certain CIP exception conditions, such as an imminent hardware failure, should necessarily trigger a relaxation of physical security protections for communications links transmitting sensitive data in all circumstances.

SDT Response: The SDT drafted the requirement with the understanding that there may be instances where a Responsible Entity may not be able to maintain compliance with the requirement as a result of a CIP Exceptional Circumstance. Responsible Entities may need to use alternate, as-yet-unidentified data transmission methods as a result of a CIP Exceptional Circumstance event. This allowance will enable Responsible Entities to focus on reliability without the risk of a compliance issue.

Control Center Definition

Several commenters expressed concerns with the proposed definition of Control Center, particularly identifying the last paragraph concerning a Generating Operator. At least one commenter stated that the use of the word "capability" is ambiguous and will confuse Registered Entities and Compliance Enforcement Authorities, and suggested the SDT consider the approved Applicability within PER-005-2 part 4.1.5.1.

SDT Response: The SDT thanks you for the comments and is continuing to work on possible revisions to the definition to address these concerns and others.

Coordination with other Entities

More than one commenter stated that the proposed standard does not make clear how entities should work together when addressing security concerns across a communication network link, and stating that, if both entities work with CIP Standard assumptions on both ends of a communication network, some support for joint handling of issues could be made clear; however, if only one entity is CIP-compliant for a given link, the current standard draft does not make clear the extent of protection expected for the data. The commenter further asked where the obligation for protecting a link per entity starts and ends.

At least one commenter stated that the proposed standard does not provide a sufficient level of detail on how entities should work together to handle security concerns across a communication network. The commenter suggested that the standard should clearly identify where the obligations for protecting data in a communication network start and end per entity.

One commenter noted that, if the region is responsible for the system, all entities would have to coordinate with the region on a solution, and that the solution may require additional equipment

to be installed. The commenter further stated that a region-wide formal agreement may be difficult to develop and execute in a year.

At least one commenter stated that implementing industry-wide secure communications is a significant coordination challenge for entities and their associated vendors. The commenter further stated that increases in security bring increased complexity, maintenance, and failure potential that may negatively impact the reliable operation of the BES. The commenter stated that, as a result, coordination for encryption key management will become an essential activity and guidance would be appreciated by stakeholders for these activities.

SDT Response: The SDT agrees with these concerns and has modified the requirement to include, "Identification of roles and responsibilities of each Responsible Entity for applying security protection to the transmission of Real-time Assessment and Real-time monitoring and control data between Control Centers, when the Control Centers are owned or operated by different Responsible Entities." This requires entities to participate in this coordination while maintaining flexibility on implementation of this requirement. The SDT has also modified the Implementation Plan to allow twenty-four (24) months to accomplish these tasks.

Exclusion in CIP-002 thru CIP-011

More than one commenter indicated that it is unclear whether the addition of proposed Reliability Standard CIP-012-1 affects the exemptions of communication networks in any of the applicability sections of other standards (CIP-002 through CIP-011). At least one commenter requested clarification that proposed Reliability Standard CIP-012-1 fills in some of the gap that the commenter asserted was created by the CIP-002 – CIP-011 third party telecommunications exemption (4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters).

SDT Response: The SDT does not intend for CIP-012 to modify the list of Cyber Assets managed under CIP-002 thru CIP-011. The SDT acknowledges that the Cyber Assets secured under CIP-002 thru CIP-011 are under the control of the Responsible Entity. The telecom equipment listed in the exemptions of these standards is to exclude equipment not under the management of the Response Entity. However, under CIP-012, the Responsible Entity does have the capability to protect the data that is transmitted across the equipment not under its control.

Implementation Guidance

Several commenters stated that Implementation Guidance for proposed Reliability Standard CIP-012-1 would be helpful.

At least one commenter suggested that without implementation guidance describing how to accomplish the required risk mitigation, it is difficult to predict the amount of time that would be required to implement this requirement part. The commenter added that they cannot assume the twelve (12) months prescribed in the proposed implementation plan is adequate.

At least one commenter indicated that it would be beneficial to have guidance on key management and inter-utility agreements particularly as it pertains to coordination for encryption of data between third parties and compliance impacts on reliability.

At least one commenter suggested guidance on the possible determination of the security method used being developed at the regional or Reliability Coordinator level to facilitate a more cost-effective approach. That same commenter also noted that Implementation Guidance could also address the entity evidence needed when an entity is following what was determined by the Region, Reliability Coordinator, or Independent System Operator.

SDT Response: The SDT is developing implementation guidance to be submitted for ERO endorsement. Specific implementation examples are being identified.

Link to IRO and TOP standards

Several commenters requested the SDT link the data to be protected from the data specifications developed under Standards TOP-003 and IRO-010, so there will be no ambiguity as to what "data" is to be protected.

At least one commenter stated that data associated with Operational Planning Analyses (OPA), Real-time monitoring (RTm), and Real-time Assessments (RTA) are predicated on other Standards and protection of data is required but all three areas (OPA, RTm, and RTA) are not subject equally to the Applicable Entities noted in CIP-012-1. That same commenter stated that the SDT, in the Technical Rationale and Justification document acknowledges TOP-003 and IRO-010 "provides consistent scoping of identified data" Based on this, the commenter suggested the SDT quantify the data to be protected is the data associated with the Applicable entities with IRO-010-2 and TOP-003-3. The commenter asserted that, by doing so, the SDT will articulate what analysis the entity is to preform and what "data" is to be protected, based on already approved NERC Reliability Standards.

SDT Response: The SDT agrees with the concerns notes and had modified Requirement R1 to only apply to Real-time Assessment and Real-time monitoring and control data. The SDT has compared the applicability of TOP-003-3 and IRO-010-1. The SDT has determined CIP-012-1 should not apply to Distribution Providers, since it is unlikely they own or operate a Control Center.

Scope of data

Several commenters expressed concern with the phrase "Real-time monitoring" as used in proposed Reliability Standard Requirement R1, since "Real-time" is defined as "present time as opposed to future time." One commenter stated that the word "monitoring" may mean ALL monitoring of an entity's entire SCADA system; however, it should be the "monitoring" of only BES data that is required for Operational Planning Analysis and Real-time Assessments.

At least once commenter stated that proposed Reliability Standard CIP-012-1 should be aligned with TOP-003-3, as data security is already required in TOP-003-3 Requirement R5. The

commenter further states that only data that is stipulated in the TOP-003-3 Requirement R1 data specification for Operational Planning Analysis, Real-time Assessment, and Real-time monitoring should be in scope for proposed Reliability Standard CIP-012-1.

One commenter stated that the NERC ORD may serve as a reference guide and resource regarding the scope of this standard and sensitive data generally, since the NERC ORD Agreement has long maintained an accepted, well-established definition for sensitive reliability data. That same commenter stated that the definition does not include data used in the Operational Planning Horizon and, for the reasons discussed above, asserts that the inclusion of Operational Planning Analysis in proposed Reliability Standard CIP-012-1 Requirement R1 extends the scope of BES sensitive data without attendant benefit to reliability. The commenter further recommended the deletion of Operational Planning Analysis from proposed Reliability Standard CIP-012-1, Requirement R1, to allow the Requirement to remain consistent with well-established, well understood precedent as set forth in the NERC ORD Agreement.

One commenter expressed concern that the scope of the standard regarding data protection (based on IRO-010 and TOP-003) extends the requirement to data/information that is not currently required to be protected at the level of a High Impact BES Cyber System, and asserted that this approach does not match the intent and protections of all other NERC CIP standards.

SDT Response: The SDT does not agree with the need to define the term "Real-time monitoring". The SDT has modified Requirement R1 to apply to Real-time Assessment and Real-time monitoring and control data. This is to be consistent with the Control Center definition which says "One or more facilities hosting operating personnel that monitor and control the Bulk Electric System (BES) in real-time." The SDT does not intend for CIP-012 to modify the list of Cyber Assets managed under CIP-002 thru CIP-011. The SDT acknowledges that the Cyber Assets secured under CIP-002 thru CIP-011 are under the control of the Responsible Entity. The communication networks and data communication links listed in the exemptions of these standards is to exclude equipment not under the management of the Response Entity. However, under CIP-012, the Responsible Entity does have the capability to protect the data that is transmitted across the equipment not under their control.

Q5 Additional Comments

One commenter states that the requirement language of proposed Reliability Standard CIP-012-1 focuses on the risk of unauthorized disclosure or modification of data, and notes that, in an operational environment the integrity and availability legs of the CIA triad are more critical than the confidentiality. The commenter suggested the SDT consider revising the proposed Reliability Standard to focus on ensuring the integrity and availability of the data.

SDT Response: The timelines for making data available through required submissions are defined within the TOP and IRO Reliability Standards. Responsible Entities are required to submit the data in order to maintain compliance with the TOP and IRO Standards. The SDT does not see the need to add to this obligation with CIP-012.

A commenter stated that Reliability Standard CIP-012-1, Requirement R2 does not identify a "reasonable" timeline for implementing the plan identified in R1, and asserted that the lack of a timeline could lead to prolonged and needless delay in implementing the required protections.

SDT Response: The SDT has also modified the Implementation Plan to allow twenty-four (24) months to accomplish these tasks.

One commenter requested clarification in the standard verbiage that the intent of this standard applies to inter control center communication.

SDT Response: The intent of the SDT is to apply the requirements to communications between Control Centers owned or operated by the same entity (intra-entity) or by different distinct entities (inter-entity).

At least one commenter asserted that Generator Operators within the ERCOT footprint who are not also Qualified Scheduling Entities (QSE) will not be able to comply with the standard as written if their Control Center transmits and receives the data as specified in proposed Reliability Standard CIP-012-1, Requirement R1. The commenter further stated that, within the ERCOT footprint, the sensitive BES data transmitted between the Control Centers of the Balancing Authority (BA), Transmission Operator (TOP), Reliability Coordinator (RC) and Generator Operator (GOP) are submitted through the QSE (Assume that ERCOT is acting as the RC, BA and/or TOP for particular GOP and that GOP is not also a QSE), and that the QSE is not a recognized NERC Functional Entity and as such would not be subject to adhering to NERC Reliability Standards. The commenter further stated that it would not be possible for a GOP to protect the sensitive BES data that is transmitted to and from the Control Center of the QSE and ERCOT that ultimately is either being sent or received by the GOP Control Center. NERC CIP-012-1, as written, does not account for this ERCOT nuance.

SDT Response: CIP-012-1 is applicable to NERC-registered Generator Operators and Generator Owners. Responsible Entities are to ensure that Real-time Assessment and Real-time monitoring and control data is protected throughout the transmission between each Control Center, regardless of any other third party in the middle of the transmission of the data. To address the concerns with coordination between Responsible Entities, modified the requirement to include, "Identification of responsibilities, when Control Centers are owned or operated by different Responsible Entities, for applying the security protection of the transmission of Real-time Assessment and Real-time monitoring and control data". This requires entities to participate in this coordination while maintaining flexibility on implementation of this requirement. The SDT has also modified the Implementation Plan to allow twenty-four (24) months to accomplish these tasks.

A commenter stated that if the SDT retains a data-centric approach, the commenter considers the time element very important and correctly captured in the requirement with the phrase "while being transmitted between Control Centers," and the commenter encouraged the SDT to

retain this language. The commenter stated the RSAW for proposed Reliability Standard CIP-012-1 does not include a time element and just says "transmitted between."
SDT Response: The SDT thanks you for your comment and has retained this concept.

One commenter stated that simply specifying that some risk mitigation should be applied by means that include physical, logical and possibly other means leads to insufficient conditions '' for establishing compliance both for the responsible entity and anyone reviewing compliance for that entity. The commenter further states that entities should consider not only that risk mitigation should take place, but also the thresholds for residual risk that should be considered acceptable for such communication.

SDT Response: The SDT thanks you for your comment and agrees with the advice noted.

At least one commenter requested that the SDT verify and confirm that the Glossary of Terms Used in NERC Reliability Standards defined terms 'Operational Planning Analyses', 'Real-time Assessments', and 'Real-time' (mentioned in the Rationale Section in reference to Requirement R1) are defined and properly aligned with the Rules of Procedure (RoP) documentation. That same commenter requested the SDT provide clarity on why the RoP is not mentioned in the Implementation Plan like the NERC Glossary of Terms. The commenter stated that the RoP, and the definitions it contains, have the same significance that the Glossary of Terms have in reference to the industry defined terms.

SDT Response: The SDT deliverables are the Standard, Implementation Plan, and definitions to be included in the NERC Glossary of Terms Used in Reliability Standards. The SDT does not have the ability to modify the Rules of Procedure.

One commenter stated that, although the FERC order specifies data between Control Centers, there is OPA, RTA, and Real-time monitoring data that is not exchanged between control centers. As examples, the commenter stated that Distribution Providers provide BES sensitive data that would not be subject the standard, and that there are numerous GOPs that do not have a control center per the definition that provide BES sensitive data which also would not subject to proposed Reliability Standard CIP-012-1. The commenter then expressed concern that the aforementioned condition creates a reliability gap since these scenarios would not be covered under the current draft of proposed Reliability Standard CIP-012-1.

SDT Response: Consistent with FERC Order No. 822, paragraph 58, the SDT intends for CIP-012 to "encompass communication links and data for intra-Control Center and inter-Control Center communications." The Standard does not apply to data transmitted between any other types of BES assets.

More than one commenter noted concerns with the use of Secure ICCP and offered thoughts on the use of alternate security protection.

A commenter noted National Infrastructure Advisory Council (NIAC) recommendation to separate communication networks be used for critical communications.

SDT Response: The SDT acknowledges these concerns and drafted the requirement to allow flexibility on implementation of this requirement. This includes addressing the security objective without being prescriptive in the protections to be applied.

One commenter asked about the representation of TO Control Centers, particularly inquiring whether or not the TO field asset box on page # 5 of Technical Rationale and Justification for CIP-012-1 document includes TO Control Centers.

SDT Response: Please see response to comments for the Technical Rational document.

A commenter suggested the SDT include the phrase "where technically feasible" to proposed Reliability Standard CIP-012-1.

SDT Response: The SDT does not agree with the need for the phrase "where technically feasible". The requirement has been written to allow flexibility on implementation of this requirement. This includes addressing the security objective without being prescriptive in the protections to be applied.

One commenter expressed concern that the protective measures developed by entities for proposed Reliability Standard CIP-012-1 could have unintended consequences, particularly identifying a concern that encryption could unacceptably slow data transmission.

SDT Response: The SDT acknowledges these concerns and drafted the requirement to allow flexibility on implementation of this requirement. This includes addressing the security objective without being prescriptive in the protections to be applied.

At least one commenter suggested the SDT change the title of the CIP-012-1 requirement to "CIP-012-1-Cyber Security – Control Center Communication Links" to align with the language in FERC Order No. 822 and the language in proposed Reliability Standard CIP-012-1, Requirement R1. The commenter asserts that the current use of the term "Networks" may be misleading because it implies a broader scope of communication.

SDT Response: The title has been changed to, "Cyber Security – Communications between Control Centers".

One commenter stated that industry-wide coordination would be necessary to successfully implement encryption for proposed Reliability Standard CIP-012-1.

SDT Response: The SDT modified the requirement to include, "Identification of roles and responsibilities of each Responsible Entity for applying security protection to the transmission

of Real-time Assessment and Real-time monitoring and control data between Control Centers, when the Control Centers are owned or operated by different Responsible Entities." This requires entities to participate in this coordination while maintaining flexibility on implementation of this requirement. The SDT has also modified the Implementation Plan to allow twenty-four (24) months to accomplish these tasks.

A commenter recommended that proposed Reliability Standard CIP-012-1, Requirement R1 VSL be "Moderate" to "High" due to the fact that Requirement R1 is a documentation requirement.

SDT Response: The SDT has modified the VSLs to be varying in degree. It should be noted that if a requirement has a single VSL, the VSL must be severe.

Consideration of Comments

Project Name:	2016-02 Modifications to CIP Standards | CIP-012-1
Comment Period Start Date:	7/27/2017
Comment Period End Date:	9/11/2017
Associated Ballot:	2016-02 Modifications to CIP Standards CIP-012-1 IN 1 ST

There were 81 sets of responses, including comments from approximately 207 different people from approximately 139 companies representing the 10 Industry Segments as shown in the table on the following pages.

All comments submitted can be reviewed in their original format on the project page.

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process. If you feel that your comment has been overlooked, or was insufficiently addressed, please let us know by contacting the Senior Director, Standards and Education, Howard Gugel (via email) or at (404) 446-9693.

Questions

1. Requirement R1: The SDT drafted CIP-012-1 Requirement R1 to meet the mandatory requirement for the Responsible Entity to develop one or more documented plan(s) to mitigate the risk of the unauthorized disclosure or modification of data used for Operational Planning Analysis, Real-time Assessment, and Real-time monitoring data while being transmitted between Control Centers. Do you agree with this revision? If not, please provide the basis for your disagreement and an alternate proposal.

2. Requirement R1: The SDT seeks comment on the need to scope sensitive BES data as it applies to Operational Planning Analysis, Real-time Assessment, and Real-time monitoring. Do you agree with scoping CIP-012-1 Requirement R1 in this manner? Please provide comment in support of your response.

3. Implementation Plan: The SDT revised the Implementation Plan such that the standard and NERC Glossary terms are effective the first day of the first calendar quarter that is twelve (12) calendar months after the effective date of the applicable governmental authority's order approving the standard, or as otherwise provided for by the applicable governmental authority. Do you agree with this proposal? If you agree with the proposed implementation time period, please note the actions you will take that require this amount of time to complete. If you think an alternate implementation time period is needed – shorter or longer - please propose an alternate implementation plan and provide a detailed explanation of actions and time needed to meet the implementation deadline.

4. The SDT believes proposed CIP-012-1 provides entities with flexibility to meet the reliability objectives in a cost effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost effective approaches, please provide your recommendation and, if appropriate, technical justification.

5. If you have additional comments on the proposed CIP-012-1 – Cyber Security -- Communication Networks drafted in response to the FERC directive that you have not provided in response to the questions above, please provide them here.

The Industry Segments are:

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

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim	3	RF	FirstEnergy Corporation	Aaron Ghdooshim	FirstEnergy - FirstEnergy Corporation	4	RF
					Aubrey Short	FirstEnergy - FirstEnergy Corporation	1	RF
					Theresa Ciancio	FirstEnergy - FirstEnergy Corporation	3	RF
					Robert Loy	FirstEnergy - FirstEnergy Solutions	5	RF
					Ann Ivanc	FirstEnergy - FirstEnergy Solutions	6	RF
Brandon McCormick	Brandon McCormick		FRCC	FMPA	Tim Beyrle	City of New Smyrna Beach Utilities Commission	4	FRCC
					Jim Howard	Lakeland Electric	5	FRCC
					Lynne Mila	City of Clewiston	4	FRCC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Javier Cisneros	Fort Pierce Utilities Authority	3	FRCC
					Randy Hahn	Ocala Utility Services	3	FRCC
					Don Cuevas	Beaches Energy Services	1	FRCC
					Jeffrey Partington	Keys Energy Services	4	FRCC
					Tom Reedy	Florida Municipal Power Pool	6	FRCC
					Steven Lancaster	Beaches Energy Services	3	FRCC
					Mike Blough	Kissimmee Utility Authority	5	FRCC
					Chris Adkins	City of Leesburg	3	FRCC
					Ginny Beigel	City of Vero Beach	3	FRCC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
Tennessee Valley Authority	Brian Millard	1,3,5,6	SERC	Tennessee Valley Authority	Scott, Howell D.	Tennessee Valley Authority	1	SERC
					Grant, Ian S.	Tennessee Valley Authority	3	SERC
					Thomas, M. Lee	Tennessee Valley Authority	5	SERC
					Parsons, Marjorie S.	Tennessee Valley Authority	6	SERC
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
MRO	Dana Klem	1,2,3,4,5,6	MRO	MRO NSRF	Joseph DePoorter	Madison Gas & Electric	3,4,5,6	MRO
					Larry Heckert	Alliant Energy	4	MRO
					Amy Casucelli	Xcel Energy	1,3,5,6	MRO
					Michael Brytowski	Great River Energy	1,3,5,6	MRO

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Jodi Jensen	Western Area Power Administration	1,6	MRO
					Kayleigh Wilkerson	Lincoln Electric System	1,3,5,6	MRO
					Mahmood Safi	Omaha Public Power District	1,3,5,6	MRO
					Brad Parret	Minnesota Powert	1,5	MRO
					Terry Harbour	MidAmerican Energy Company	1,3	MRO
					Tom Breene	Wisconsin Public Service Corporation	3,5,6	MRO
					Jeremy Voll	Basin Electric Power Cooperative	1	MRO
					Kevin Lyons	Central Iowa Power Cooperative	1	MRO
					Mike Morrow	Midcontinent ISO	2	MRO

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
SERC Reliability Corporation	David Greene	10	SERC	SERC CIPC	Bill Peterson	SERC RRO	10	SERC
					Mike Hagee	SERC RRO	10	SERC
					SERC CIPC	Various	1,2,5,9	SERC
Con Ed - Consolidated Edison Co. of New York	Dermot Smyth	5	NPCC	Con Edison	Dermot Smyth	Con Edison Company of New York	1,3,5,6	NPCC
					Edward Bedder	Orange & Rockland		NPCC
Seattle City Light	Ginette Lacasse	1,3,4,5,6	WECC	Seattle City Light Ballot Body	Pawel Krupa	Seattle City Light	1	WECC
					Hao Li	Seattle City Light	4	WECC
					Bud (Charles) Freeman	Seattle City Light	6	WECC
					Mike Haynes	Seattle City Light	5	WECC
					Michael Watkins	Seattle City Light	1,4	WECC
					Faz Kasraie	Seattle City Light	5	WECC
					John Clark	Seattle City Light	6	WECC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Tuan Tran	Seattle City Light	3	WECC
					Laurrie Hammack	Seattle City Light	3	WECC
Santee Cooper	James Poston	3		Santee Cooper	Rene' Free	Santee Cooper	1	SERC
					Rodger Blakely	Santee Cooper	1	SERC
					Chris Jimenez	Santee Cooper	1	SERC
					Troy Lee	Santee Cooper	1	SERC
					Tom Abrams	Santee Cooper	1	SERC
					Jennifer Richards	Santee Cooper	1	SERC
					Stony Martin	Santee Cooper	1	SERC
					Glenn Stephens	Santee Cooper	1	SERC
					Tom Perry	Santee Cooper	1	SERC
Lower Colorado River Authority	Michael Shaw	1		LCRA Compliance	Teresa Cantwell	LCRA	1	Texas RE
					Dixie Wells	LCRA	5	Texas RE
					Michael Shaw	LCRA	6	Texas RE
Southern Company - Southern	Pamela Hunter	1,3,5,6	SERC	Southern Company	Katherine Prewitt	Southern Company Services, Inc.	1	SERC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
Company Services, Inc.					R. Scott Moore	Alabama Power Company	3	SERC
					William D. Shultz	Southern Company Generation	5	SERC
					Jennifer G. Sykes	Southern Company Generation and Energy Marketing	6	SERC
Eversource Energy	Quintin Lee	1		Eversource Group	Timothy Reyher	Eversource Energy	5	NPCC
					Mark Kenny	Eversource Energy	3	NPCC
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,8,9,10	NPCC	RSC no Con-Edison and Dominion	Guy V. Zito	Northeast Power Coordinating Council	10	NPCC
					Randy MacDonald	New Brunswick Power	2	NPCC
					Wayne Sipperly	New York Power Authority	4	NPCC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					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	Orange & Rockland Utilities	3	NPCC
					Michele Tondalo	UI	1	NPCC
					Laura Mcleod	NB Power	1	NPCC
					Michael Schiavone	National Grid	1	NPCC
					Michael Jones	National Grid	3	NPCC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					David Ramkalawan	Ontario Power Generation Inc.	5	NPCC
					Quintin Lee	Eversource Energy	1	NPCC
					Kathleen Goodman	ISO-NE	2	NPCC
					Greg Campoli	NYISO	2	NPCC
					Silvia Mitchell	NextEra Energy - Florida Power and Light Co.	6	NPCC
					Paul Malozewski	Hydro One Networks, Inc.	3	NPCC
					Sylvain Clermont	Hydro Quebec	1	NPCC
					Helen Lainis	IESO	2	NPCC
					Chantal Mazza	Hydro Quebec	2	NPCC
Dominion - Dominion Resources, Inc.	Sean Bodkin	6		Dominion	Connie Lowe	Dominion - Dominion Resources, Inc.	3	NA - Not Applicable
					Lou Oberski	Dominion - Dominion	5	NA - Not Applicable

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
						Resources, Inc.		
					Larry Nash	Dominion - Dominion Virginia Power	1	NA - Not Applicable
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
					Deborah McEndaffer	Midwest Energy, Inc.	NA - Not Applicable	SPP RE
					Don Schmit	Nebraska Public Power District	5	SPP RE

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Louis Guidry	Cleco Corporation	1,3,5,6	SPP RE
					Robert Hirchak	Cleco Corporation	6	SPP RE
					Marty Paulk	Cleco Corporation	1,3,5,6	SPP RE
					Michelle Corley	Cleco Corporation	3	SPP RE
					Robert Gray	Board of Public Utilities	NA - Not Applicable	SPP RE
					Ron Spicer	EDP Renewables	NA - Not Applicable	SPP RE
					Steven Keller	Southwest Power Pool	2	SPP RE
					Laura Cox	Westar Energy	5	SPP RE
PPL - Louisville Gas and Electric Co.	Shelby Wade	3,5,6	RF,SERC	Louisville Gas and Electric Company and Kentucky Utilities Company	Charles Freibert	PPL - Louisville Gas and Electric Co.	3	SERC
					Dan Wilson	PPL - Louisville Gas and Electric Co.	5	SERC
					Linn Oelker	PPL - Louisville Gas and Electric Co.	6	SERC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
PSEG	Sheranee Nedd	1,3,5,6	NPCC,RF	PSEG REs	Tim Kucey	PSEG - PSEG Fossil LLC	5	RF
					Karla Jara	PSEG Energy Resources and Trade LLC	6	RF
					Jeffrey Mueller	PSEG - Public Service Electric and Gas Co	3	RF
					Joseph Smith	PSEG - Public Service Electric and Gas Co	1	RF
ACES Power Marketing	Warren Cross	1,3,4,5	MRO,RF,SERC,SPP RE,Texas RE,WECC	ACES Standards Collaborators	Arizona Electric Power Cooperative, Inc.	AEPC	1	WECC
					Hoosier Energy Rural Electric Cooperative, Inc.	HE	1	RF
					Sunflower Electric Power Corporation	SEPC	1	SPP RE

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Rayburn Country Electric Cooperative	RCEC	3	SPP RE
					Old Dominion Electric Cooperative	ODEC	3,4	SERC
					Brazos Electric Power Cooperative, Inc.	BRAZOS	1,5	Texas RE
					Southern Maryland Electric Cooperative	SMECO	3	RF
					North Carolina Electric Membership Corporation	NCEMC	3,4,5	SERC
					Central Iowa Power Cooperative	CIPCO	1	MRO
					East Kentucky Power Cooperative	EKPC	1,3	SERC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Buckeye Power, Inc.	BUCK	4	RF

1. ***Requirement R1: The SDT drafted CIP-012-1 Requirement R1 to meet the mandatory requirement for the Responsible Entity to develop one or more documented plan(s) to mitigate the risk of the unauthorized disclosure or modification of data used for Operational Planning Analysis, Real-time Assessment, and Real-time monitoring data while being transmitted between Control Centers. Do you agree with this revision? If not, please provide the basis for your disagreement and an alternate proposal.***	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	
Comment	
The term “transmitted between Control Centers” is not clear. Dominion is concerned that the demarcation point between Control Centers is unclear and could cause confusion? A second concern is the potential reliability gap created by the lack of a clarification on whether internal Control Center communications networks are considered to be part of the transmission of data, or if only external communications between entities qualify as transmission data?	
Likes 0	
Dislikes 0	
Response	
George Brown - Acciona Energy North America - 5	
Answer	No
Document Name	
Comment	

The term “plan” is misleading in this context. A “plan” is more analogous to the development of a project that has actions to achieve a result by specific date; similar to an implementation plan for a NERC Reliability Standard. If it was the intention of the SDT to require a Responsible Entity to have a documented set of requirements to protect the sensitive BES data transmitted between the Control Centers then the term “policy” would be more appropriate. A policy is interpreted to be more dynamic and ongoing throughout the lifetime of the requirement. Additionally, as cyber security technology is constantly changing and evolving, a policy would allow for a definite course of action for a Responsible Entity to protect sensitive BES data transmitted between the Control Centers.	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino	
Answer	No
Document Name	
Comment	
It is an overwhelming task to differentiate what is or what isn’t confidential communication data over data links between Control Centers. As such, it is recommended that ALL data transmitted between Control Center be protected. The standards should just address all data communication between control centers. Technologies such as encryption are generally implemented by link, not communication type.	
Likes 0	
Dislikes 0	

Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	

The IESO agrees with the creation of a new standard, rather than expanding CIP-003, CIP-005 and/or CIP-006 requirements to provide new controls over physical communication links. Specifically, the IESO commends the SDT for recognizing that not all utilities own or control their own physical communications links.

The IESO offers the following comments and recommendations.

- R1. For data used for Operational Planning Analysis, Real-time Assessments, and Real-time monitoring, as documented by a Reliability Coordinator, Transmission Operator, or Balancing Authority, the Responsible Entity shall develop one or more documented plan(s) to mitigate the risk of the unauthorized disclosure or modification of the data while it is being transmitted between Control Centers. This excludes oral communications, regardless of transport means.
- The note to R1 concerning the existence of a Control Center or specified data should be a dealt with in Section 4 – Applicability part of the Standard. This would eliminate the need for this to be discussed as part of the RSAW.
- Recommend that it be clarified whether this is a standalone Standard similar to CIP-014 or if it is intended to define the scope of applicable systems to be protected under CIP-003 thru CIP-011.
- In order to evaluate the extent and kind of obligation involved, the definition of between control centers needs to be clearer with regard to the communication link. The Standard should address the proper demarcation points for obligation to show implementation and compliance. To clearly define the obligation of Responsible Entities, the required plan should include identification of the demarcation points. Information is also needed on the explicit agreements required on each end of the physical communication link to arrange and identify such demarcation. Where there is disagreement on how protections are to be applied between two or more Responsible Entities, what is the arbitration process to resolve these disagreements?

• How is the situation handled where a Responsible Entity (e.g., an RC) is receiving information from a third-party provider that is aggregating and submitting data on behalf of one or more Responsible Entities (e.g., a TOP)? What is the identification of the demarcation points? In reading the standard, it does not appear that the connection to the third-party provider is in scope since they are not a Responsible Entity or even registered with NERC. The same situation may be present for entities that use an outsourced data center provider. The question is also relevant for the data that is provided to regulatory agencies that are not bound by CIP Standards.	
Likes 2	Hydro One Networks, Inc., 1, Farahbakhsh Payam; Hydro One Networks, Inc., 3, Malozewski Paul
Dislikes 0	
Response	
Dermot Smyth - Con Ed - Consolidated Edison Co. of New York - 5, Group Name Con Edison	
Answer	No
Document Name	
Comment	
The scope of the term “data” is unclear. Does “data” apply to all data or just machine to machine (e.g. automated) communications? If it is all data would emails/ftp/etc. be in scope?	
Likes 0	
Dislikes 0	
Response	
Brandon McCormick - Brandon McCormick On Behalf of: Ginny Beigel, City of Vero Beach, 3; Lynne Mila, City of Clewiston, 4; Tom Reedy, Florida Municipal Power Pool, 6; - Brandon McCormick, Group Name FMPA	
Answer	No

Document Name	
Comment	
FMPA does not agree with the revision of Requirement 1 (R1) because the obligation is not clear. The R1 note - "If the Responsible Entity does not have a Control Center or it does not transmit the type of data specified in Requirement R1 of CIP-012-1 between two Control Centers, the requirements in CIP-012-1 would not apply to that entity."- should be in the Section 4 Applicability. This would eliminate the need for this to be discussed as part of the RSAW. In order to evaluate the extent and kind of obligation involved with R1, the phrase "transmitted between two control centers," needs to be clearer. FMPA believes that there should be more clarity or identification on the demarcation points of the link being protected. Both TOP-003 and IRO-010 have a requirement that there be a mutually agreeable security protocol. It is not clear why a new standard needs to be developed to address this same issue. The SDT should consider modifying TOP-003 and IRO-010 if these standards do not provide adequate language to meet Order No. 822's concerns.	
Likes 0	
Dislikes 0	
Response	
Frank Pace - Central Hudson Gas & Electric Corp. - 1	
Answer	No
Document Name	
Comment	
There is a lack of language within the Requirement that specifies the demarcation point for compliance between applicable Control Centers.	
Likes 0	

Dislikes 0	
Response	
Donald Lock - Talen Generation, LLC - 5	
Answer	No
Document Name	
Comment	
The applicability of the expression, “between Control Centers,” does not appear to be restricted to transmittals between Control Centers owned by a single entity; exchanges between GO and TO/TOP Control Centers would be covered also, for example. This makes sense as regards achieving a high degree of security, but could create confusion regarding who is responsible for inter-entity transmittals. CIP-012-1 should state that GO/GOP obligations for inter-entity exchanges between Control Centers are fulfilled if they follow the data specifications provided by the other party (ref. IRO-010-2 and TOP-003-3).	
Likes 0	
Dislikes 0	
Response	
David Rivera - New York Power Authority - 3	
Answer	No
Document Name	
Comment	
1. The Note to R1 concerning the existence of a Control Center or specified data should be a dealt with in Section 4 – Applicability. This would eliminate the need for this to be discussed as part of the RSAW. 2. In order to evaluate the extent and kind of obligation involved, the definition of between control centers needs to be more clear with regard to the communication link. What are the demarcation points for obligation to show compliance?	

3. Request clarification does the 15 minute impact CIP-002 identification of BES Cyber Systems affect the applicability of CIP-012?	
Likes 0	
Dislikes 0	
Response	
Philip Huff - Arkansas Electric Cooperative Corporation - 3	
Answer	No
Document Name	
Comment	
The Requirement should only permit the option to logically protect the data during transmission or at least remove the explicit options to physically protect the data. We understand the Requirement is consistent with CIP-006 R1.10, but this Requirement addresses communication lines within the same facility, and for which physical protection is possible. Cryptography is the only mechanism available to protect data across geographically dispersed Control Centers. Stating other options is confusing and has a strong potential to guide the industry toward ineffective solutions. However, if the intent is to allow physical protection of communications of Control Centers in the same geographical location, then make it clear in the Technical Guidelines the scenarios and alternative solutions the drafters had in mind.	
Likes 0	
Dislikes 0	
Response	
Jennifer Hohenshilt - Talen Energy Marketing, LLC - 6	
Answer	No
Document Name	

Comment
The applicability of the expression, “between Control Centers,” does not appear to be restricted to transmittals between Control Centers owned by a single entity; exchanges between GO and TO/TOP Control Centers would be covered also, for example. This makes sense as regards achieving a high degree of security, but could create confusion regarding who is responsible for inter-entity transmittals. CIP-012-1 should state that GO/GOP obligations for inter-entity exchanges between Control Centers are fulfilled if they follow the data specifications provided by the other party (ref. IRO-010-2 and TOP-003-3).

Likes 0	
Dislikes 0	

Response

Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	No
Document Name	

Comment
As mentioned by the SDT, FERC directs *that “…require responsible entities to implement controls to protect, at a minimum, communication links and sensitive bulk electric system data communicated between bulk electric system Control Centers…”*. First, having a plan does not add to the reliability of protecting said data. This is an unwarranted layer of compliance that is not needed. Everything does not need a plan in order to be protected. Recommend that R1 be written in parallel to the FERC directive, which does not require a plan (per the SDTs Consideration of Issues and Directives). If “Plan” is maintained in CIP-012-1 then, the SDT should explain what is meant by having a Plan? Per CIP-003-6 it states, The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter. Is a plan the template document which is used throughout our Standards or is it a set of controls that show that the data is being protected per R1? The NSRF does not understand why a Plan is needed when the data is being protected by physical or electronic means. If a Plan is

required, then all the Plan is going to say is that the cabling that transfers data is in a protected conduit (or other means) between Control Centers. Secondly, The NSRF questions why the SDT is not in line with the FERC Order to "…protect …data…" but the proposed R1 states to "…mitigate the risk of unauthorized disclosure or modification of data…"? R1 should be rewritten to state: "The responsible entity shall have controls (or other understandable words) in place to protect against the unauthorized disclosure or modification of BES data used for Operational Planning Analysis, Real-time Assessments, and Real-time monitoring while being transmitted between BES Control Centers. This excludes oral communications". Please note that the word "BES" is needed within R1 regardless of it our proposed rewrite is accepted or not.

Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	No
Document Name	
Comment	

Texas RE appreciates the Standard Drafting Team's (SDT) efforts to develop a workable approach to mitigate the risk of unauthorized disclosure or modification of certain categories of Control Center communications. However, Texas RE is concerned that the proposed CIP-012-1 R1 does not fully satisfy the directives established by the Federal Energy Regulatory Commission (FERC) in FERC Order No. 822. Texas RE is likewise concerned that the proposed CIP-012-1 may not adequately address third-party entities handling sensitive data between Control Centers in the Texas RE region.

First, throughout its discussion concerning new requirements for protecting Control Center communications, FERC emphasized that additional protections were required to protect both the "integrity and availability of sensitive bulk electric system data." FERC Order No. 822, P. 54. FERC made clear that this involved, at a minimum, two discrete actions. First, FERC stressed that entities should implement

controls to protect the physical communications links transmitting sensitive data between Control Centers. Second, FERC noted that the sensitive data itself needed to be protected to ensure its accuracy and consistency. In issuing the directive underpinning this rulemaking, FERC stated: "we adopt the NOPR proposal and direct that NERC . . . develop modifications to the CIP Reliability Standards to require responsible entities to implement controls to protect, at a minimum, communications links and sensitive bulk electric system data communicated between bulk electric system Control Centers . . . FERC Order No. 822, P. 53 (emphasis added).

FERC made it clear that protections should apply to both communication links and sensitive data. However, the proposed draft of CIP-012-1 R1 potentially applies only to physical protections for communications links or to logical protections for data during its transmission. That is, responsible entities could simply elect to plan and implement physical protections for communications links. This would "mitigate" the risk of an unauthorized disclosure or modification of data using one of the delineated methods. As such, the responsible entity would potentially be compliant with the Standard without proposing or implementing any logical protections for sensitive data during its transmission. This appears counter to FERC's intent to protect "both the integrity and availability of sensitive bulk electric system data." FERC Order No. 822, P. 54.

Second, Texas RE is concerned that the proposed CIP-012-1 standard may result in confusion, particularly among Generation Operators with Control Centers subject to the standard regarding the scope of their compliance obligations or, alternatively, may inadvertently result in a significant reliability gap given the structure of the ERCOT market. In ERCOT, generators do not communicate directly with the regional Reliability Coordinator (ERCOT). Instead, generators are required to communicate through designated entities known as Qualified Scheduling Entities (QSEs). In many instances, these QSEs are third-party entities. Within the NERC regulatory construct, Generator Operators have delegated certain NERC compliance functions to these entities, including providing data used for Operational Planning Analysis, Real-time Assessments, and Real-time monitoring. Critically, Generator Operators remain responsible for all compliance obligations associated with QSE activities in the ERCOT region.

In light of this market and regulatory framework, Texas RE interprets the proposed draft of CIP-012-1 to likewise require Generator Operators possessing Control Centers to take steps to mitigate the risk of unauthorized data disclosures at every step along the communication chain between its Control Center and the ERCOT Control Center, including steps to protect this data at third-party intermediary QSEs. Otherwise, the proposed draft of CIP-012-1 would result in a significant reliability gap as QSE communications links and data passing from the QSE to ERCOT could be potentially unsecure. Given this fact, Generator Operators will likely need to take steps to ensure that their third-party QSEs have accorded designated sensitive data appropriate protections, which could in turn require incorporating such requirements into QSE agreements or other steps. Texas RE requests the SDT clarify that communications between QSEs (or equivalent in other Regions) and the RC are subject to CIP-012-1 requirements and that Responsible Entities must take steps to

address mitigate the risk of unauthorized data disclosures for these communications as well in order to ensure that Responsible Entities have sufficient notice of these compliance obligations.	
Likes 0	
Dislikes 0	
Response	
Alice Wright - Arkansas Electric Cooperative Corporation - 4	
Answer	No
Document Name	2016-02_CIP-012-1_Comment_Form_07272017-AECC Comments.pdf
Comment	
See attachment	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	No
Document Name	
Comment	
See APPA Comments.	
Likes 0	

Dislikes 0	
Response	
James Poston - Santee Cooper - 3, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	
Recommend removing "Operational Planning Analysis" from this requirement. Operational Planning Analysis is not Real-time data and would not affect the BES within 15 minutes. The TOP-003-3 Standard currently requires a mutually agreeable security protocol for sharing of data required for Operational Planning Analyses.	
Likes 0	
Dislikes 0	
Response	
Marty Hostler - Northern California Power Agency - 5	
Answer	No
Document Name	
Comment	
NCPA does not feel CIP-012-1 is needed as both TOP-003 R5 and IRO-010 R3 require Registered Entities (REs) to use a mutually agreeable security protocol. The SDT should consider modifying TOP-003 and IRO-010 if these standards do not provide adequate language to meet Order No. 822's concerns. Also please refer to other APPA, TAPs, and Utility Services comments.	
Likes 0	

Dislikes 0	
Response	
Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	
Comment	
NCPA does not feel CIP-012-1 is needed as both TOP-003 R5 and IRO-010 R3 require Registered Entities (REs) to use a mutually agreeable security protocol. The SDT should consider modifying TOP-003 and IRO-010 if these standards do not provide adequate language to meet Order No. 822's concerns. Also please refer to other APPA, TAPs, and Utility Services comments.	
Likes 0	
Dislikes 0	
Response	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	No
Document Name	
Comment	
The applicability section of the Standard should specify that the requirements only apply to entities with Control Centers. This would allow the elimination of the note to R1 and would simplify the ERO monitoring process.	
Likes 0	
Dislikes 0	

Response	
Heather Morgan - EDP Renewables North America LLC - 5	
Answer	No
Document Name	
Comment	
What does, “Physically protecting the communication links transmitting the data,” mean? A Registered Entity is able to physically protect its end point, but is not able to physically protect the communication link for the entire communication link. Please define “logical protection” to provide clarification for entities for implementation and compliance oversight. What does, “Using an equally effective method to mitigate the risk of unauthorized disclosure or modification of the data” mean?	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	No
Document Name	
Comment	
The Purpose section of CIP-012-1 adds the need to protect the confidentiality of data which is out of Scope of FERC order 822. Although it is recognized that the SDT is not limited to just FERC orders, adding need to protect the confidentiality of data does not add reliability if the data is being protected per CIP-012-1 R1.	
Likes 0	

Dislikes 0	
Response	
Aaron Austin - AEP - 3	
Answer	No
Document Name	
Comment	
AEP suggests that a new requirement(s) be added to establish a hierarchy for REs that requires entities at the top with the most risk to set the communications security protocols. And, modify the existing R1 to require REs to have plans that follow the protocols set by the entities identified in the new requirement(s).	
Likes 0	
Dislikes 0	
Response	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	No
Document Name	
Comment	

1. The Note to R1 concerning the existence of a Control Center or specified data should be a dealt with in Section 4 – Applicability. This would eliminate the need for this to be discussed as part of the RSAW.
2. In order to evaluate the extent and kind of obligation involved, the definition of between control centers needs to be more clear with regard to the communication link. What are the demarcation points for obligation to show compliance?

3. Request clarification does the 15 minute impact CIP-002 identification of BES Cyber Systems affect the applicability of CIP-012?

4. Concerns exist with the relationships regarding implementation of CIP-012 with other NERC Standards such as IRO, TOP, CIP-006 R1 Part1.10

Likes 0	
Dislikes 0	

Response

Lona Calderon - Salt River Project - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

SRP requests the SDT consider differentiating requirements for Control Center communications within an entity from those for Control Center communications between entities. Because data being sent for TOP-003 and IRO-010 traverses over the ICCP network maintained by a carrier, entities cannot provide physical protections for communication of this data from end to end. In this case, protecting the confidentiality and integrity can only be done through encryption. However, since no one utility owns the hardware end to end on the ICCP network, site to site encryption cannot be implemented. The only options available would be application layer encryption or transport layer encryption utilizing IEC 62351-4 Secure ICCP.

For IRO-010 data, the RC in the Western Interconnect requires real-time data to be sent every 10 seconds. Likewise, For TOP-003 data, SRP is required to send and receive real-time data every 10 seconds to and from various other entities on the ICCP network within the Western Interconnect. It is unclear the amount of latency that may be added or amount of computing resources required to encrypt and decrypt this data every 10 seconds. Additionally, the RC would be receiving this data from all applicable utilities in the Western Interconnect. If all entities encrypt and send data every 10 seconds, it is unclear how much latency would be added and computing resources would be required by the RC to decrypt the large amount data. It is also unclear how the added latency would affect the real-time operations of the Bulk Electric System. IRO and TOP data specification changes may be necessary to address delays in data due to latency, or process/procedure changes to mitigate effects on real-time operations. SRP suggests performing a study or survey to

determine how much data is being sent and received and what the effects would be from the added latency and the amount of extra computing resources required. SRP requests clarification on the exclusion of oral communications. Additionally, SRP suggests the exclusion for oral communications be expanded to also exclude electronic mail. SRP requests clarification for what would be accepted as physical security either in the measures or Technical Rationale and Justification. SRP also requests clarification of what equally effective methods are in the measures or Technical Rationale and Justification.	
Likes 0	
Dislikes 0	
Response	
Thomas Breene - WEC Energy Group, Inc. - 3	
Answer	No
Document Name	
Comment	
As mentioned by the SDT, FERC directs *that "…require responsible entities to implement controls to protect, at a minimum, communication links and sensitive bulk electric system data communicated between bulk electric system Control Centers…"*. First, having a plan does not add to the reliability of protecting said data. This is an unwarranted layer of compliance that is not needed. Everything does not need a plan in order to be protected. Recommend that R1 be written in parallel to the FERC directive, which does not require a plan (per the SDTs Consideration of Issues and Directives). If "Plan" is maintained in CIP-012-1 then, the SDT should explain what is meant by having a Plan? Per CIP-003-6 it states, The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter. Is a plan the template document which is used throughout our Standards or is it a set of controls that show that the data is being protected per	

R1? We do not understand why a Plan is needed when the data is being protected by physical or electronic means. If a Plan is required, then all the Plan is going to say is that the cabling that transfers data is in a protected conduit (or other means) between Control Centers. Secondly, we question why the SDT is not in line with the FERC Order to "…protect …data…" but the proposed R1 states to "…mitigate the risk of unauthorized discloser or modification of data…"? R1 should be rewritten to state: "The responsible entity shall have controls (or other understandable words) in place to protect against the unauthorized disclosure or modification of BES data used for Operational Planning Analysis, Real-time Assessments, and Real-time monitoring while being transmitted between BES Control Centers. This excludes oral communications". Please note that the word "BES" is needed within R1 regardless of it our proposed rewrite is accepted or not.	
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 agrees with and support the comments submitted by the MRO Standards Review Forum (NSRF) in regards to this question.	
Likes 0	
Dislikes 0	
Response	
Russell Noble - Cowlitz County PUD - 3	

Answer	No
Document Name	
Comment	
Cowlitz PUD supports the comments submitted by APPA.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Con-Edison and Dominion	
Answer	No
Document Name	
Comment	
· The Note to R1 concerning the existence of a Control Center or specified data should be a dealt with in Section 4 – Applicability. This would eliminate the need for this to be discussed as part of the RSAW. · In order to evaluate the extent and kind of obligation involved, the definition of between control centers needs to be clearer with regard to the communication link. What are the demarcation points for obligation to show compliance? · Request clarification does the 15 minutes impact CIP-002 identification of BES Cyber Systems affect the applicability of CIP-012?	
Likes 0	
Dislikes 0	
Response	

Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	

ERCOT ISO signs on to the ITC SWG comments:

The ITC SWG agrees with the creation of a new standard, rather than expanding CIP-003, CIP-005 and/or CIP-006 requirements to provide new controls over physical communication links. Specifically, the ITC SWG commends the SDT for recognizing that not all utilities own or control their own physical communications links.

The ITC SWG offers the following comments and recommendations.

- R1. For data used for Operational Planning Analysis, Real-time Assessments, and Real-time monitoring, as documented by a Reliability Coordinator, Transmission Operator, or Balancing Authority, the Responsible Entity shall develop one or more documented plan(s) to mitigate the risk of the unauthorized disclosure or modification of the data while it is being transmitted between Control Centers. This excludes oral communications, regardless of transport means.
- The note to R1 concerning the existence of a Control Center or specified data should be a dealt with in Section 4 – Applicability part of the Standard. This would eliminate the need for this to be discussed as part of the RSAW.
- Recommend that it be clarified whether this is a standalone Standard similar to CIP-014 or if it is intended to define the scope of applicable systems to be protected under CIP-003 thru CIP-011.
- In order to evaluate the extent and kind of obligation involved, the definition of between control centers needs to be clearer with regard to the communication link. The Standard should address the proper demarcation points for obligation to show implementation and compliance. To clearly define the obligation of Responsible Entities, the required plan should include identification of the demarcation points. Information is also needed on the explicit agreements required on each end of the physical communication link to arrange and identify such demarcation. Where there is disagreement on how protections are to be applied between two or more Responsible Entities, what is the arbitration process to resolve these disagreements?

- How is the situation handled where a Responsible Entity (e.g., an RC) is receiving information from a third-party provider that is aggregating and submitting data on behalf of one or more Responsible Entities (e.g., a TOP)? What is the identification of the demarcation points? In reading the standard, it does not appear that the connection to the third-party provider is in scope since they are not a Responsible Entity or even registered with NERC. The same situation may be present for entities that use an outsourced data center provider. The question is also relevant for the data that is provided to regulatory agencies that are not bound by CIP Standards.

Likes 0	
Dislikes 0	
Response	
Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 3	
Answer	No
Document Name	
Comment	
Tacoma Power suuports the commetns of APPA	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1	
Answer	No
Document Name	Project 2016-02_CIP-012-1_NSRF Final.docx
Comment	

WAPA agrees with the comments submitted by the NSRF (attached)	
Likes 0	
Dislikes 0	
Response	
Theresa Rakowsky - Puget Sound Energy, Inc. - 1	
Answer	No
Document Name	
Comment	
See APPA Comments.	
Likes 0	
Dislikes 0	
Response	
Jack Cashin - American Public Power Association - 4	
Answer	No
Document Name	
Comment	
APPA does not agree with the revision of Requirement 1 (R1) because the obligation is not clear. The R1 note - “If the Responsible Entity does not have a Control Center or it does not transmit the type of data specified in Requirement R1 of CIP-012-1 between two Control	

Centers, the requirements in CIP-012-1 would not apply to that entity."- should be in the Section 4 Applicability. This would eliminate the need for this to be discussed as part of the RSAW.

Evaluation of the extent and kind of obligation involved with R1, requires a clearer phrase than, "transmitted between two control centers." Public power believes that there should be more clarity or identification on the demarcation points of the link being protected.

Both TOP-003 and IRO-010 have a requirement that there be a mutually agreeable security protocol. It is not clear why a new standard needs to be developed to address this same issue. The SDT should consider modifying TOP-003 and IRO-010 if these standards do not provide adequate language to meet Order No. 822's concerns.

Likes 0	
Dislikes 0	

Response

Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	No
Document Name	

Comment

CenterPoint Energy Houston Electric, LLC ("CenterPoint Energy") recommends adding more clarification on the scope of the term "communication links." Data used for Operational Planning Analysis (OPA), Real-time Assessments (RTA), and Real-time monitoring (RTM) is collected based on an Entity-issued data specification, per TOP-003-3 and IRO-010-2. This data is collected through a medium referred to as "data exchange capability," as required by TOP-001-4 (Requirements R19 and R20) as well as IRO-002-5 (Requirements R1 and R2).

OPA data is typically not transmitted via a communication link, and OPA data presents lower risk to operations than real-time telemetry data exchanged via ICCP communication links between Control Centers. The systems used to transmit the OPA data can be located outside Control Centers and are not considered BES Cyber Systems since they do not impact the Bulk Electric System within 15 minutes. Thus, CenterPoint Energy believes OPA data should not be within the scope of Requirement R1.

In addition to removing OPA from Requirement R1, CenterPoint Energy recommends revising Requirement R1 to include the term “inter and intra Control Center communication links.” This revision aligns with the language in Federal Energy Regulatory Commission (“FERC”) Order No. 822. The proposed revised language is below: “The Responsible Entity shall develop one or more documented plan(s) to mitigate the risk of the unauthorized disclosure or modification of data used for Real-time Assessments and Real-time monitoring while being transmitted between **inter and intra** Control Centers **communication links**. This excludes oral communications.”	
Likes 0	
Dislikes 0	
Response	
Warren Cross - ACES Power Marketing - 1,3,4,5 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standards Collaborators	
Answer	No
Document Name	
Comment	
(1) We agree with the direction of the requirement, however, the wording of the “one of more of” phrase seems to be in conflict with the intention of physical and logical protection. How can you protect the data without physical security, and how can you ensure data integrity without logical protection? The “one or more of” reference should be stricken. (2) We recommend the addition of wording that clearly excludes Low impact Entities from compliance with this requirement. Would a low impact control room which communicates with a Control Center be out of scope? (3) We propose moving the compliance applicability note that follows Requirement R1 to the applicability section of the standard, particularly Section 4.2 Exemptions.	
Likes 0	
Dislikes 0	

Response	
Michael Puscas - ISO New England, Inc. - 2	
Answer	No
Document Name	
Comment	
In order to evaluate the extent and kind of obligation involved, the definition of between control centers needs to be clearer with regard to the communication link. What are the demarcation points for obligation to show compliance? Should there be explicit agreements with each end of the communication link to arrange such demarcation? How should responsible entities deal with third parties involved with trust relationships in communication links (i.e. telecommunications providers managing routers)?	
Likes 0	
Dislikes 0	
Response	
David Greyerbiehl - CMS Energy - Consumers Energy Company - 5	
Answer	No
Document Name	
Comment	
The requirement as written does not provide clear definition on what type of data needs to be protected, and how exactly the physical/logical protection approach should be accomplished.	
Likes 0	
Dislikes 0	

Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	

BPA appreciates the revisions that the SDT has made based on industry feedback on the SAR.

BPA reiterates its position as documented in our SAR comments that CIP-012-1 is not necessary.

Alternate proposal #1: The objectives can be met by coordinating with existing standards such as CIP-003 and CIP-005.

If CIP-012-1 moves forward, there are areas requiring clarification. FERC Order No. 822 requires implementation of controls to protect, at a minimum, communication links AND sensitive BES data communicated between BES Control Centers. However, the SDT is providing latitude to protect communication links, data or both. If it is an "AND" as stated in Order No. 822, it is not always technically feasible to implement both controls to protect communication links and sensitive BES data communicated between BES Control Centers.

Points of discussion:

Implementation of controls to protect the data:

- Encryption may not be feasible due to availability concerns. (e.g., failure of encryption keys or latency problems with encryption for availability requirements.)

Implementation of controls on communication links:

- The use of the term communication links may be broadly interpreted and difficult to audit.
- It may not be technically feasible to implement physical controls, for example:

- on fiber optic cable on power lines
- on a common carrier system where the links are unknown
- for wireless communications - how does an entity physically protect the air between endpoints?

Additionally, entities and common carriers use a variety of media to carry traffic, and will undoubtedly use traffic shaping to maintain service levels: routing becomes unpredictable; each packet could take a different route from point A to B.

If an entity owns the communication network from end to end, this is still a problem. Modern routing protocols will try to deliver packets over a system with inoperable equipment, severed links, etc. The only remedy is to physically protect the entire communication system in advance of system faults to satisfy CIP-012. If one packet traverses a link due to a system fault that is not protected – it would be a violation.

If FERC agrees with the SDT's proposal of allowing the entity the latitude to protect the data, communication links or both, BPA believes the security objective will not be met. BPA recommends placing controls on the data AND **end points** where technically feasible. However BPA recommends moving R1.1 to a Technical Guidance, considering there are multiple implementation methods for controls on data and end points.

Likes 0	
Dislikes 0	
Response	
James Anderson - CMS Energy - Consumers Energy Company - 1	
Answer	No
Document Name	
Comment	

The requirement as written does not provide clear definition on what type of data need to be protected, and how exactly the physical/logical protection approach should be accomplished by an entity.	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	No
Document Name	
Comment	
Utility Services does not agree with the revision of Requirement 1 (R1) because the obligation is not clear. The R1 note - "If the Responsible Entity does not have a Control Center or it does not transmit the type of data specified in Requirement R1 of CIP-012-1 between two Control Centers, the requirements in CIP-012-1 would not apply to that entity."- should be in the Section 4 Applicability. This would eliminate the need for this to be discussed as part of the RSAW. In order to evaluate the extent and kind of obligation involved with R1, the phrase "transmitted between two control centers", needs to be clearer. Public power believes that there should be more clarity or identification on the demarcation points of the link being protected. Both TOP-003 and IRO-010 have a requirement that there be a mutually agreeable security protocol. It is not clear why a new standard needs to be developed to address this same issue. The SDT should consider modifying TOP-003 and IRO-010 if these standards do not provide adequate language to meet Order No. 822's concerns.	
Likes 0	
Dislikes 0	
Response	

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No
Document Name	
Comment	

Southern Company has concerns with the phrase “data used for Operational Planning Analysis, Real-time Assessments, and Real-time monitoring” in CIP-012 R1. We understand this is a direct quote from TOP-003 R1 and IRO-010 R1 and the intent is for this phrase to point to the data specification required by those standards. We understand there is a paragraph to this effect in the Technical Rationale document which is not a binding document. Our concern is that the requirement says “data used for…” and without a stronger bind to the IRO and TOP standards we believe this opens the scope of CIP-012 to yet another data definition exercise rather than a specific requirement to protect an already defined data specification while that data is being transferred between Control Centers.

The draft RSAW for R1 puts this concern in writing. It does not instruct the auditor to use the specifications from TOP-003/IRO-010 Requirement 1 and verify that this previously defined data is protected while being transferred between Control Centers. Instead it requires the auditor to verify

“The documented plan(s) collectively address all data used for Operational Planning Analysis, Real-time Assessments, and Real-time monitoring transmitted between Control Centers”

It then includes glossary definitions for two of those terms. The auditor is instructed to look at two definitions, determine a definition of the undefined “Real-time monitoring”, and then verify that all such data is protected. This effort alone dwarfs the true purpose of the standard which is protecting those communications links over which BES Control Centers communicate system status with each other in real time.

We suggest an alternative to resolve this issue. First, we suggest that a data centric approach is problematic for these and other reasons and we strongly suggest a more technical approach that focuses CIP-012 on securing communication sessions and/or links based on their destination. For example, data that is leaving the ESP or LEAP of a Control Center that has a destination address of an ESP or LEAP at another Control Center should be encrypted. That is very distinct and concrete and much simpler to implement and demonstrate and we believe is in line with FERC Order 822, paragraph 60 where the Commission outlines the reliability gap to be addressed.

If this alternative is not acceptable, we suggest that R1 be modified to make the previously defined data specification the noun rather than "data used for…". Additionally, we suggest removing "Operational Planning Analysis" from the first paragraph of R1 as Operational Planning Analysis data does not impact the BES within 15 minutes.

For example: *"The Responsible Entity shall develop one or more documented plan(s) to mitigate the risk of the unauthorized disclosure or modification of data used for Real-time Assessments and Real-time monitoring* ***as specified by the Reliability Coordinator or Transmission Operator*** *while* ***such data*** *is being transmitted between Control Centers. This excludes oral communications."*

We also strongly suggest, based on questions in the draft RSAW, that the SDT consider moving any language relating to applicability to the Applicability section of the standard rather than having a note in the requirement language. With the inclusion of the note in the requirement, we notice the draft RSAW starts with questions for all the responsible entities that do not have Control Centers to prove the negative, which should instead defer any auditor to the compliance auditing process of CIP-002-5.1.

Likes 0	
Dislikes 0	

Response

Ronald Donahey - TECO - Tampa Electric Co. - 3

Answer	No
Document Name	

Comment

Tampa Electric Company suggests that the SDT provide additional instruction within the standard to address the requirements and implications for BA's that serve as the BA for other entities in the BA's service area. It would be helpful to understand the BA's responsibility to mitigate the risk of unauthorized disclosure or modification of data used for the analysis, assessment and monitoring. In addition, does this standard extend to communications between a Registered Entities and the Reliability Coordinators such as FRCC's RC in relation to communication between Control Centers?

Likes 0	

Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	No
Document Name	
Comment	

The SPP Standards Review Group has reviewed documentation and have developed some concerns in reference to Requirement R1. The CIP Version 5 Transition Advisory Group (V5TAG) identified specific issues with the CIP Version 5 standard language that caused difficulty in implementation of the requirements. This requirement or a supplemental to CIP-005 needs to clarify 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 or a single ESP. This should be address either in this standard, as an Exemption added or requirement added to CIP-005-6.

Here is proposed language for the Exemption:

4.2.3. Exemptions: The following are exempt from Standard CIP-002-5.1:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety

Commission.

4.2.3.2. *Exemption of Communication Equipment that is owned and operated by a Third Party Communication Carrier or its equivalent is exempted from the CIP standards that is communicating between system end points*

Cyber Assets associated with communication networks and data (striking this information)

communication links between discrete Electronic Security Perimeters. (striking this information)

Or added to CIP-005-6 R1

CIP-005-5 Table R1 – Electronic Security Perimeter

Part

1.6

Applicable

High Impact BES Cyber Systems and their associated:

- *PCA*

Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:

- *PCA*

Requirements

For defined ESPs that use wide-area communications networks (e.g. ESPs that span multiple geographic locations), Cyber Assets associated with communication networks and data communication links used to facilitate the ESP and owned by a third party are exempt from the CIP Reliability Standards provided that the communications traversing across these Cyber Assets are encrypted. The Cyber Assets that encrypt and decrypt the communications are EACMS.

Measures

An example of evidence may include, but is not limited to, network diagrams showing all communication networks, vendor owned equipment, and encryption/decryption Cyber Assets.

There are two major reasons for addressing this issue listed above. 1) This was identified by the V5TAG group and can be easily fixed with one of the two suggestions listed above. Reason 2) is because Registered Entities may expand their ESP's to cover both control centers to handle R1.1 in regards of:

- *Logically protecting the data during transmission; or (Provide example or measures)*

- *Using a measurements to mitigate the risk of unauthorized disclosure or modification of the data.*

Likes 0	
Dislikes 0	

Response

Wendy Center - U.S. Bureau of Reclamation - 5

Answer	No
Document Name	

Comment

Reclamation recommends the SDT use the term “documented processes” consistently throughout the CIP standards. Pursuant to CIP-003-6,

The terms program and plan are sometimes used in place of documented processes where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as plans (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Reclamation disagrees that having a plan adds to the reliability of protecting data used for Operational Planning Analysis, Real-time Assessment, and Real-time monitoring. A plan is an unwarranted layer of compliance that is not needed. Reclamation recommends that R1 be written in parallel with the FERC Order 822, which directed the development of controls to protect communication links and data. Reclamation recommends R1 could be rewritten to state: “The responsible entity shall have documented processes in place to mitigate the risk of the unauthorized disclosure or modification of **BES** data used for Operational Planning Analysis, Real-time Assessments, and Real-time monitoring while being transmitted between BES Control Centers. This excludes oral communications.” Reclamation recommends that the word “BES” be added to R1 regardless of whether the SDT accepts the rest of the above proposed language.

If the requirement for a plan is retained, Reclamation recommends the SDT clarify what is meant by having a plan and how a plan is different from a documented process.

Reclamation recommends using the following definitions of “plan” and “process:” *Plan: Written account of intended future course of action (scheme) aimed at achieving specific goal(s) or objective(s) within a specific timeframe. It explains in detail what needs to be done, when, how, and by whom, and often includes best case, expected case, and worst case scenarios. See also planning.* *Process: Sequence of interdependent and linked procedures which, at every stage, consume one or more resources (employee time, energy, machines, money) to convert inputs (data, material, parts, etc.) into outputs. These outputs then serve as inputs for the next stage until a known goal or end result is reached.*	
Likes 0	
Dislikes 0	
Response	
Scott Berry - Scott Berry On Behalf of: Jack Alvey, Indiana Municipal Power Agency, 1, 4; - Scott Berry	
Answer	No
Document Name	
Comment	
We have attached our comments in the last question for the definition of Control Center. We are recommending changes to this definition.	
Likes 0	
Dislikes 0	
Response	
Lauren Price - American Transmission Company, LLC - 1	

Answer	No
Document Name	
Comment	

ATC believes the language should be in better alignment with the directives of the FERC order to establish a plan and implement controls to address the risks posed to the BES. ATC also believes the requirement language should be less prescriptive as it relates to data types. ATC believes the Requirement language must allow an appropriate level of flexibility for Registered Entities to identify and document the risks posed to the BES and the corresponding data to assure implemented controls are (and remain) commensurate with risk. The requirement should be focused on the achievement and ongoing sustainability of the security objective in order to permit adaption of their plan(s) and the associated implemented controls such that they are designed to effectively address the current and emerging risks posed to BES Control Center assets and information as the threat landscape changes. Some potential language for consideration is:

"R1. For sensitive Bulk Electric System (BES) data communicated between BES Control Centers, Responsible Entities shall establish and implement one or more documented plans that collectively identifies and addresses:

R1.1. the communication links capable and purposed for the transport of BES data between BES Control Centers

R1.2. the risks posed to the BES from the transport of the BES data between BES Control Centers

R1.2. the BES data subject to the risk

R1.3. the protective measures and security practices designed and implemented to mitigate the identified risks.

R1.4. the process and cycle to review and update the plan(s) to maintain alignment with risks posed

BES data excludes oral communications."

Likes 0	
Dislikes 0	
Response	

James Gower - Entergy - NA - Not Applicable - SERC	
Answer	No
Document Name	
Comment	
The standard as drafted explicitly excludes oral communications, but does not consider forms of written communication (email, chat, etc) that could communicate the same type of information that an oral communication could. These written instructions are commonly outside of SCADA systems and are on corporate systems, and this standard would require physical or logical controls on those systems for communications that may traverse these systems. The standard should specify the protection of "operational data", "BCS Data", or some other term to clarify protection of data outside of instructions, or provide data validation (i.e verify emails by phone) as an acceptable control. Additionally, Entergy has concerns over expanding the scope of protection from "real-time" as defined in other CIP standards and through existing CIP definitions, to require the protection of Operational Planning Analysis data that is outside of the "real-time" horizon. Requests additional clarity regarding whether the protection is required for data that is used to an input to Operational Planning Analysis, or also includes Operational Planning Analysis data outputs. The Technical Justification and Rationale document seems to imply it is data inputs as it calls out data believed to already be within BES Cyber Systems.	
Likes 0	
Dislikes 0	
Response	
Guy Andrews - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	

- GSOC (Georgia Systems Operations Corporation) requests that the Standards Drafting team provide formal CIP-012 Guidance and Technical Basis (GTB) or Implementation Guidance, either within the Standard or as separate documentation. This is crucial for an entity's understanding of how to meet the compliance objective of a new Standard.
- GSOC requests clarification regarding:
- he applicability of the Standard to TOs. This Standard should apply only TOs who own or operate Control Centers. An example of modifying the applicability can be found in MOD-025-2.
- the precise nature of Operator-to-Operator communications. "Oral Communications" are excluded. However, EOP-008 (Emergency Operating) Plans often specify using cell/text/email while in mid-failover to the backup site. Would these types of communications also be excluded?
- The Rationale talks about "CIP-012-1 Requirements R1 and R2 protections for applicable data during transmission between two **geographically** separate Control Centers." However, the requirements themselves don't seem to make that same distinction. Since the definition of a "Control Center" includes associated data centers, this could lead to the application of this Standard, for example, to a facility that houses 2 control centers side-by-side (one with a data center downstairs). GSOC requests that the Drafting Team provide more information about the Rationale, as it relates to geographical location and proximity of Control Centers, and corresponding language of the Requirements.
- CIP-012 includes protections for data while being transmitted between Control Centers. However, Control Centers are facilities and do not transmit data. Does this include only data transmitted between BES Cyber Systems associated with a Control Center or data transmitted by certified System Operators?

Likes 0	
Dislikes 0	
Response	
Laura McLeod - NB Power Corporation - 5	
Answer	No
Document Name	
Comment	

TOP-003/IRO-010 both require applicable entities have mutual agreement on security protocols. This mutual agreement requirement text of TOP-003/IRO-010 may limit or prevent an entity from following its documented plans of CIP-012-1 R1 should, as an example, either entity change its security protocols.

One approach is to also include the requirement for mutual agreement within CIP-12-1 and/or be more prescriptive in how an entity complies with CIP-012-1 R1 including coordination between entities.

Likes 0	
Dislikes 0	

Response

Annette Johnston - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3

Answer	No
Document Name	

Comment

We do not agree with two separate requirements, one for a plan and one to implement. We recommend following precedent in the other CIP standards, for example, CIP-004-011. The obligation can be accomplished with one requirement, such as follows, with the caveat of concerns expressed in question 1 about what data is covered.

The Responsible Entity shall implement one or more documented processes(s) to mitigate the risk of the unauthorized disclosure or modification of data used for Operational Planning Analysis, Real-time Assessments, and Real-time monitoring while being transmitted between Control Centers, except under CIP Exceptional Circumstances . This excludes oral communications. Risk mitigation shall be accomplished by one or more of the following actions: (follow with the four bullets).

Delete R2.

With one requirement, the note could be simpler by not referencing "R1 of CIP-012-1" and "CIP-012-1." See following.

Note: If the Responsible Entity does not have a Control Center or it does not transmit the type of data specified in this Requirement between two Control Centers, this Requirement would not apply to that entity.	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	
Comment	
See MidAmerican Energy Company comments.	
Likes 0	
Dislikes 0	
Response	
Laurie Williams - PNM Resources - Public Service Company of New Mexico - 1	
Answer	No
Document Name	
Comment	
The requirement is too general and would likely not yield consistent compliance among entities and would result in inconsistent auditing of compliance.	

Likes 0	
Dislikes 0	
Response	
Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 3	
Answer	No
Document Name	
Comment	
The requirement is too general and would likely not yield consistent compliance among entities and would result in inconsistent auditing of compliance	
Likes 0	
Dislikes 0	
Response	
Haley Sousa - Public Utility District No. 1 of Chelan County - 5	
Answer	No
Document Name	
Comment	
CHPD requests clarification be added to the Technical Rationale for acceptable means of physically protecting communications links and identifying equally effective methods to mitigate risk. CHPD requests that the exclusion for oral communications be extended to electronic mail.	

Likes 0	
Dislikes 0	
Response	
Janis Weddle - Public Utility District No. 1 of Chelan County - 6	
Answer	No
Document Name	
Comment	
CHPD requests clarification be added to the Technical Rationale for acceptable means of physically protecting communications links and identifying equally effective methods to mitigate risk. CHPD requests that the exclusion for oral communications be extended to electronic mail.	
Likes 0	
Dislikes 0	
Response	
David Greene - SERC Reliability Corporation - 10, Group Name SERC CIPC	
Answer	No
Document Name	3B-2016-02_CIP-012-1_Unofficial_Comment_Form_CIPC.docx
Comment	
Likes 0	
Dislikes 0	

Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
TVA agrees, providing the proposed definition of Control Center is adopted. TVA notes that in many cases some types of operational planning analysis data is housed in systems not classified as BES Cyber Systems and may not reside within an ESP. A documented plan provides a mechanism to identify and document flows of BES sensitive data that do not originate from within an ESP nor pass through an EAP.	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
IPC does not agree with the need for mandatory requirements. IPC evaluates risks and develops strategies to mitigates those risks, including those associated with communication infrastructure and data transmission. Risks can change, and the implementation of static regulatory obligations that are not flexibly written can make it more difficult to adapt.	
Likes 0	

Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	

Even though ReliabilityFirst votes in the affirmative, ReliabilityFirst provides the following comments for consideration:

1. Requirement R1 –

    i. CIP-012-1 refers to data as outlined in NERC standards TOP-003-3 and IRO-010-2 that are required to be protected. ReliabilityFirst understands these types of data can vary based on entity function and what data is needed. From a compliance monitoring perspective, it may be difficult to verify what the entity is protecting versus what actually should be protected. ReliabilityFirst requests the SDT to consider putting a list of typical data that should be protected per the standard and include it in a guideline document or rationale section.

    ii. The standard, as written, states "Risk mitigation shall be accomplished by one or more of the following actions: Physically protecting the communication links transmitting the data; Logically protecting the data during transmission; or Using an equally effective method to mitigate the risk of unauthorized disclosure or modification of the data." Since this is data in transit (over the "air") ReliabilityFirst inquires on how one provides physical protections? In addition to this, the selection of encryption cyphers, and key lengths are not required. ReliabilityFirst suggests to place some language about encryption in a "technical basis", explaining that there are different cyphers, some better than others, and after weighing the pros and cons of different cyphers and key lengths recommend the use of site-to-site IPV6 encapsulation with a specific cypher and key length.

Likes 0	
Dislikes 0	

Response	
Chris Scanlon - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon agrees with the approach of the latest revision, which provides latitude to protect the communication links, the data, or both, to satisfy the security objective consistent with the capabilities of the Responsible Entity's operational environment. We do, however, question the placement of the "Note" portion within R1. The Note applies not just to R1, but to CIP-012-1 as a whole. Is there a reason for not including this under Section 4 Applicability, as an exemption?	
Likes 0	
Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 3	
Answer	Yes
Document Name	2016-02 Modifications to CIP Standards CIP-012-1 - Answer to Question 1.docx
Comment	
Please see the attached document for Arizona Public Service Co.'s answer to Question 1.	
Likes 0	
Dislikes 0	

Response	
Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	Yes
Document Name	
Comment	
NRECA agrees with the construct of the standard and its requirements, but not the scope of sensitive BES data as detailed in the response to question 2.	
Likes 0	
Dislikes 0	
Response	
Shelby Wade - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company	
Answer	Yes
Document Name	
Comment	
We support SERC's comments.	
Likes 0	
Dislikes 0	
Response	

David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
OPG has concerns with potential issues arising from communication links not owned by entity. Potential issues can also occur when the communication is performed between the CC belonging to different entities; how is the demarcation point determined.	
Likes 0	
Dislikes 0	
Response	

Mark Riley - Associated Electric Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
AECI agrees with the construct of the standard and its requirements, but not the scope of sensitive BES data as detailed in the response to question 2.	
Likes 0	
Dislikes 0	
Response	

RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
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	
Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Shannon Fair - Colorado Springs Utilities - 1,3,5,6, Group Name Colorado Springs Utilities	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 3, Group Name FirstEnergy Corporation	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sheranee Nedd - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	
Likes 1	PSEG - PSEG Fossil LLC, 5, Kucey Tim

Dislikes 0	
Response	
Michael Shaw - Lower Colorado River Authority - 1, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb On Behalf of: Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 3, 5, 1, 6; James McBee, Great Plains Energy - Kansas City Power and Light Co., 3, 5, 1, 6; Jessica Tucker, Great Plains Energy - Kansas City Power and Light Co., 3, 5, 1, 6; Jim Flucke, Great Plains Energy - Kansas City Power and Light Co., 3, 5, 1, 6; - Douglas Webb	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	

Answer	
Document Name	
Comment	
The California ISO supports the comments of the Security Working Group (SWG).	
Likes 0	
Dislikes 0	
Response	

2. *Requirement R1: The SDT seeks comment on the need to scope sensitive BES data as it applies to Operational Planning Analysis, Real-time Assessment, and Real-time monitoring. Do you agree with scoping CIP-012-1 Requirement R1 in this manner? Please provide comment in support of your response.*

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	
Comment	
See MidAmerican Energy Company comments.	
Likes 0	
Dislikes 0	
Response	

Annette Johnston - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	No
Document Name	
Comment	
The FERC directive refers to "sensitive bulk electric system data" and directs NERC to "identify the scope of sensitive build electric system data." The FERC directive also acknowledges that certain entities are already required to exchange necessary real-time and operational planning data through secured networks using mutually agreeable security protocol. Draft Requirement 1 refers to "data used for Operational Planning Analysis, Real-time Assessments, and Real-time monitoring." We agree with other commenters that these references require revision. Further, we ask the SDT to consider scoping sensitive data explicitly to	

information exchanged between Control Centers' BES Cyber Systems. This corresponds to SDT's assertation that "this data resides within BES Cyber Systems, and while at rest is protected by CIP-003 through CIP-011." It also corresponds to FERC's recognition of mutually agreeable security protocol networks referenced above.	
Likes 0	
Dislikes 0	
Response	
Laura McLeod - NB Power Corporation - 5	
Answer	No
Document Name	
Comment	
Since Operational Planning Analysis is not real-time data and since planning data/information is generally scrutinized when performing analysis the risk of acting on corrupted data (entry error or unauthorized disclosure/modification) is low.	
Likes 0	
Dislikes 0	
Response	
Mark Riley - Associated Electric Cooperative, Inc. - 1	
Answer	No
Document Name	
Comment	

AECI contends that data used for Operational Planning Analysis (OPA) is not sensitive BES data and does not have a 15 minute impact on the reliable operation of the BES. The CIP standards focus on span of control of BES Cyber Systems and their impact to the reliable operation of the BES. Data used for Real-time Assessments and Real-time monitoring can immediately impact the reliable operation of the BES, but data used for OPA has no such impact. AECI requests that the SDT remove OPA from R1 due to not impacting the reliable operation of the BES.	
Likes 0	
Dislikes 0	
Response	
James Gower - Entergy - NA - Not Applicable - SERC	
Answer	No
Document Name	
Comment	
Entergy has concerns over expanding the scope of protection from “real-time” as defined in other CIP standards and through existing CIP definitions, to require the protection of Operational Planning Analysis data that is outside of the “real-time” horizon.	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 5	
Answer	No
Document Name	

Comment
Reclamation recommends adding “BES” data to the language as stated above in question 1.

Likes 0	
Dislikes 0	

Response

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group

Answer	No
Document Name	

Comment
The SPP Standards Review Group has a concern that the scope doesn’t provide the appropriate coverage of the BES data. We would like to propose some new language to address those potential concerns. First of all, a “plan” does not necessarily mean the data is protected. According to the Rationale section FERC is looking for controls to protect these communication links. It should also be clarified that this is “BES” data. The SDT, in the Technical Rationale and Justification document acknowledges TOP-003-3 and IRO-010-2 “provides consistent scoping of identified data” [R1 section: Alignment with IRO and TOP Standards”]. We believe that the data specifications under TOP-003-3 R1 and IRO-010-2 R1 correctly scope the data to be protected; however the current R1 only leaves us with three defined terms for scoping. These 3 defined terms were already used to scope the data specifications under TOP-003-3 R1 and IRO-010-2 R1. CIP-012-1 R1 should reference to TOP-003-1 R1 and IRO-010-2 R1. We realize that it is not the preferred method to reference another Standard; however since CIP-012 is classified as a CIP Standard, and not an Operations and Planning Standard which would be the correct classification, CIP auditors may expand the data to be protected based solely on definitions. In order to properly scope CIP-012, it should reference the TOP-003 and IRO-010 Standards.

R1 should be re-written: “The Responsible Entity shall have controls in place to mitigate the risk of the unauthorized disclosure or modification of BES data identified under entity developed data specifications in TOP-003-3 R1 for applicable entities and IRO-010-2 R1 for applicable entities; while such data is being transmitted between BES Control Centers. This excludes oral communications.”	
Likes 0	
Dislikes 0	
Response	
Ronald Donahey - TECO - Tampa Electric Co. - 3	
Answer	No
Document Name	
Comment	
Please provide additional clarification on the protection of load forecasting data as it may not consistently be included as a separate BES Cyber System.	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No
Document Name	
Comment	

As per the concern noted in response to question 1, we agree that either further clarification on the scope of the data is needed so it is clear the data in question has already been scoped and is in specifications that are required by IRO-010 and TOP-003, or the SDT should consider setting aside a “data-centric” approach and focus protections on a more technical solution regardless of the data being transmitted between Control Center ESPs and LEAPs.

Likes 0	
Dislikes 0	

Response

Brian Evans-Mongeon - Utility Services, Inc. - 4

Answer	No
Document Name	

Comment

Utility Services does not agree with the scope of the CIP-012-1 R1 as it applies to Operational Planning Analysis, Real-time Assessment, and Real-time monitoring. Since Operational Planning Analysis data would not meet the 15-minute impact criteria used in the identification of BES Cyber Systems, this data would only be required to be protected as it is being transmitted between Control Centers. This inconsistency between the data systems identified by CIP-012-1 and those identified in other CIP standards may cause the unintended expansion of scope of the CIP Standards.

Public power believes applying controls to the Operational Planning Analysis data may reduce the current ability of entities to share this data which may cause a reduction in BES reliability. Not all of this data goes from Control Center to Control Center but may go to (or from) a location outside of a Control Center and therefore would not be in scope of the drafted CIP-012 standard. USI suggests removing the Operational Planning and Analysis data from the scope of this standard.

If the Operational Planning and Analysis data must be retained in the Standard, then USI believes that an exemption for the communication of Operational Planning and Analysis data by email should be put in place. This would be similar to the exemption that exists for voice communication.

Likes 0	
Dislikes 0	
Response	
James Anderson - CMS Energy - Consumers Energy Company - 1	
Answer	No
Document Name	
Comment	
The requirement suggested data are different from those protected in other CIP standards. This may cause confusion in the future by calling it a CIP standard.	
Likes 0	
Dislikes 0	
Response	
David Greyerbiehl - CMS Energy - Consumers Energy Company - 5	
Answer	No
Document Name	
Comment	
The requirement suggested data are different from those protected in other CIP standards. This may cause confusion in the future by calling it a CIP standard.	
Likes 0	
Dislikes 0	

Response	
Warren Cross - ACES Power Marketing - 1,3,4,5 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standards Collaborators	
Answer	No
Document Name	
Comment	
We disagree with the inclusion of Operational Planning Analysis (OPA) based on its NERC definition, as these evaluations are assessed on anticipated and potential conditions for next-day operations and outside the 15-minute impact on the reliable BES operations. The inclusion of OPA is unnecessary and the technical basis does not support it being in scope because it is not impacting the BES in real time.	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	
CenterPoint Energy believes not all data included in OPA, RTA, and RTM is sensitive BES data. CenterPoint Energy recommends the SDT narrow the scope further to only sensitive BES data. Some inputs into OPAs, RTAs, and RTMs (e.g. forecast type data, modeling data such as Facility Ratings, phase angle limitations, etc.) should not be included in the scope of this project. On a situational basis, some telemetry and outage information would also not be considered sensitive BES data.	

CenterPoint Energy further recommends that OPA data be completely removed from the scope of CIP-012-1. CenterPoint Energy does not deem this data to be considered sensitive BES data, nor does this data carry the significance of actual Real-time data used for RTAs and RTM.	
Likes 0	
Dislikes 0	
Response	
Jack Cashin - American Public Power Association - 4	
Answer	No
Document Name	
Comment	

APPA does not agree with the scope of the CIP-012-1 R1 as it applies to Operational Planning Analysis, Real-time Assessment, and Real-time monitoring. Since Operational Planning Analysis data would not meet the 15-minute impact criteria used in the identification of BES Cyber Systems, this data would only be required to be protected as it is being transmitted between Control Centers. This inconsistency between the data systems identified by CIP-012-1 and those identified in other CIP standards may cause the unintended expansion of scope of the CIP Standards.

Public power believes applying controls to the Operational Planning Analysis data may reduce the current ability of entities to share this data which may cause a reduction in BES reliability. Not all of this data goes from Control Center to Control Center but may go to (or from) a location outside of a Control Center and therefore would not be in scope of the drafted CIP-012 standard. APPA suggests removing the Operational Planning and Analysis data from the scope of this standard.

If the Operational Planning and Analysis data must be retained in the Standard, then APPA believes that an exemption for the communication of Operational Planning and Analysis data by email should be put in place. This would be similar to the exemption that exists for voice communication.

An important consideration with respect to scope and data protection, is the impact encryption may have on the data being considered within the scope of the standard. As SRP communicates in their comments: until the implications are understood about the amount of data being considered for the standard and the impact of encryption on latency and computing resources, the scope may be over-reaching. Therefore, APPA believes that the scoping for the standard does not sufficiently take these factors into account.	
Likes 0	
Dislikes 0	
Response	
Theresa Rakowsky - Puget Sound Energy, Inc. - 1	
Answer	No
Document Name	
Comment	
See APPA Comments.	
Likes 0	
Dislikes 0	
Response	
Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 3	
Answer	No
Document Name	
Comment	

Tacoma Power supports the comments of APPA	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	No
Document Name	
Comment	
While we agree with the SDTs approach to align with TOP-003 and IRO-010, we feel that technologies such as encryption or physical protection are generally implemented by link, not communication type.	
Likes 0	
Dislikes 0	
Response	
Russell Noble - Cowlitz County PUD - 3	
Answer	No
Document Name	
Comment	
Cowlitz PUD supports the comments submitted by APPA.	

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 is concerned with the inclusion of BES data used for Operation Planning Analysis that does not have a 15 minute impact on the Bulk Electric System. The inclusion of Operational Planning Assessment data would bring corporate communication links, such as corporate email, into the scope of NERC Standards.

We are also concerned with the language in Requirement R1.1 which states that a method of risk mitigation could be done by "Physically protecting the communication links transmitting data." Xcel Energy believes that the proposed standard does not define what physical controls would be sufficient to mitigate the undefined risk of "unauthorized disclosure of modification of data." Many communication devices owned by Xcel Energy reside in company facilities that have several layers of physical protection. However, once communication links leave our enclosures and ownership purview, physical protection would be difficult at best, largely unknown, and impossible to enforce. The implementation of physical controls only covers a small section of the medium for the data and does not actually protect the data itself. As one of three options; if an organization elects to impement physical controls it would still leave a gap in data integrity and add little benefit with excessive administrative burden.

Xcel Energy respectfully proposes the recommendation for physcial protection to be removed and require logical controls such as encryption, firewalls, information protection release standards and password requirements. Logical controls would more sufficiently protect the data itself end-to-end. We suggest the following edits to R1;

The Responsible Entity shall develop **and implement controls** *[strikethrough:* one or more documented plan(s)] to mitigate the risk of the unauthorized disclosure of or modification to **BES** data used for Operational Planning Analysis, Real-time Assessments, and Real-time

monitoring while being transmitted between Control Centers **and which could have an adverse impact on the BES within 15 minutes**. This excludes verbal communications. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. Risk mitigation shall be accomplished by one or more of the following actions:

- [strikethrough: Physically protecting the communication links transmitting the data;]
- Logically protect[strikethrough:ing] the data during transmission; or
- Use[strikethrough:ing] an equally effective method to mitigate the risk of unauthorized disclosure or modification of the data.

Likes 0	
Dislikes 0	
Response	

Thomas Breene - WEC Energy Group, Inc. - 3	
Answer	No
Document Name	
Comment	

The SDT needs to add “BES” data into the language as recommended above in question 1. The “BES data” to be protected should be identified as that “BES data” which can have an impact via high and medium BES Cyber Systems within 15 minutes. In other words, this level of protection should be limited to High and Medium Control Centers and only that data which could put Real-time operations at risk.

Likes 0	
Dislikes 0	
Response	

Lona Calderon - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
SRP agrees this data should be protected. However, after further discussions within SRP and with other entities in the industry, it is clear no one in the industry can state or has an understanding of the implications encryption would have on reliable operation of the BES and the data within this scope. Until a survey or evaluation is performed to understand the amount of data this scope applies to and the impact of encryption on latency and computing resources, the scope may be over-reaching. As such, the manner used for scoping does not adequately take these factors into account.	
Likes 0	
Dislikes 0	
Response	

Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	No
Document Name	
Comment	
NRECA contends that data used for Operational Planning Analysis (OPA) is not sensitive BES data and does not have a 15 minute impact on the reliable operation of the BES. The CIP standards focus on span of control of BES Cyber Systems and their impact to the reliable operation of the BES. Data used for Real-time Assessments and Real-time monitoring can immediately impact the reliable operation of the BES, but data used for OPA has no such impact. We request that the SDT remove OPA from R1 due to not impacting the reliable operation of the BES.	
Likes 0	

Dislikes 0	
Response	
Aaron Austin - AEP - 3	
Answer	No
Document Name	
Comment	
AEP suggests that "Operational Planning and Analysis" be removed from R1.	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	No
Document Name	
Comment	
The Purpose section of CIP-012-1 adds the need to protect the confidentiality of data which is out of Scope of FERC order 822. Although it is recognized that the SDT is not limited to just FERC orders, adding need to protect the confidentiality of data does not add reliability if the data is being protected per CIP-012-1 R1.	
Likes 0	
Dislikes 0	
Response	

Vivian Vo - APS - Arizona Public Service Co. - 3	
Answer	No
Document Name	
Comment	

AZPS respectfully submits that achieving a consensus regarding categorization of data as sensitive across all three interconnections will be difficult – if not impossible – to achieve. The sensitivity of the same data can vary drastically between interconnections and entities within each interconnections. For example, a piece of information that AZPS considers critical and sensitive to its real-time assessments may be viewed as insignificant to another entity. Additionally, certain markets require publication of data that other markets would consider sensitive. Hence, any attempted categorization may conflict with regulatory requirements in Open Access Transmission Tariffs, Market Protocols, state and federal regulations, etc. that obligate entities to disclose and/or that require confidentiality and that are already effective.

Furthermore, such a classification may not matter in practice. The reality is that data flows to Control Centers across a limited number of communication channels. Consider a simplified control center that uses only ICCP for real-time monitoring and assessment, with only half of the data transmitted across that channel being considered "sensitive." It is unlikely that any entity would reasonably determine that it should separate out the sensitive data for protection and leave the non-sensitive data unprotected. It is more likely that they would, instead, protect the entire communication channel. Consequently, AZPS does not support the need or see any benefit to an effort focused on scoping sensitive BES data. Instead, it recommends that responsible entities retain the authority to designate specific data or communication links as "sensitive."

Finally, in the event that the SDT determines a need to scope sensitive BES data, AZPS suggests striking the term "Operational Planning Analysis" from the requirement and limiting the data considered as sensitive to that data which is subject to the NERC Operating Reliability Data (ORD) Agreement. The NERC ORD Agreement is intended to ensure the confidentiality of sensitive data and the definition of Operating Reliability Data and associated obligations included therein are clear, well-established, and well-understood by industry. Importantly, the definition of ORD excludes "Operational Planning Analysis," signaling that such data has not, historically, been considered as "sensitive." Moreover, the Operational Planning Analysis occurs in the next day horizon, providing entities with time to receive and review data prior to use and, where data is suspect, request verification of data or, where data is not timely received, request that such data be re-transmitted. For these reasons, the data utilized in Operational Planning Analyses has extremely limited impact on

reliability, which is highly dependent on accurate, appropriate real-time data. Hence, protecting data used in real-time assessment and monitoring as has been required by the NERC ORD Agreement for years is appropriate and the scope of such data has already been evaluated for sensitivity and confidentiality. In summary, if the SDT is compelled to scope sensitive data, to ensure consistency, AZPS recommends that the SDT interpret "sensitive BES data" as encompassing data used in Real-time Assessment and Real-time monitoring only and utilize the NERC ORD Agreement as its primary reference.	
Likes 0	
Dislikes 0	
Response	
Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	
Comment	
NCPA does not agree with the scope of the CIP-012-1 as it applies to Operational Planning Analysis, Real-time Assessment, and Real-time monitoring. Since Operational Planning Analysis data would not meet the 15-minute impact criteria used in the identification of BES Cyber Systems, this data would only be required to be protected as it is being transmitted between Control Centers. This inconsistency between the data systems identified by CIP-012-1 and those identified in other CIP standards may cause the unintended expansion of scope of the CIP Standards. Also see other APPA and Utility Services/TAPs comments.	
Likes 0	
Dislikes 0	
Response	
Marty Hostler - Northern California Power Agency - 5	
Answer	No

Document Name	
Comment	
NCPA does not agree with the scope of the CIP-012-1 as it applies to Operational Planning Analysis, Real-time Assessment, and Real-time monitoring. Since Operational Planning Analysis data would not meet the 15-minute impact criteria used in the identification of BES Cyber Systems, this data would only be required to be protected as it is being transmitted between Control Centers. This inconsistency between the data systems identified by CIP-012-1 and those identified in other CIP standards may cause the unintended expansion of scope of the CIP Standards. Also see other APPA and Utility Services/TAPs comments.	
Likes 0	
Dislikes 0	
Response	
James Poston - Santee Cooper - 3, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	
Recommend removing “Operational Planning Analysis” from this requirement. Operational Planning Analysis is not Real-time data and would not affect the BES within 15 minutes. The TOP-003-3 Standard currently requires a mutually agreeable security protocol for sharing of data required for Operational Planning Analyses.	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	

Answer	No
Document Name	
Comment	
See APPA Comments.	
Likes 0	
Dislikes 0	
Response	
Alice Wright - Arkansas Electric Cooperative Corporation - 4	
Answer	No
Document Name	
Comment	
See attachment	
Likes 0	
Dislikes 0	
Response	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	No
Document Name	
Comment	

The SDT needs to add “BES” data into the language as recommended above in question 1.	
Likes 0	
Dislikes 0	
Response	
Jennifer Hohenshilt - Talen Energy Marketing, LLC - 6	
Answer	No
Document Name	
Comment	
The question is unclear.	
Likes 0	
Dislikes 0	
Response	
Philip Huff - Arkansas Electric Cooperative Corporation - 3	
Answer	No
Document Name	
Comment	
Please provide additional guidance on the scope of the information. The Standards from which the scope derives does not provide guidance, and the expansion of scope in CIP-012-1 to all Control Centers necessitates the need for more specific guidance.	

Likes 0	
Dislikes 0	
Response	
Donald Lock - Talen Generation, LLC - 5	
Answer	No
Document Name	
Comment	
The question is unclear.	
Likes 0	
Dislikes 0	
Response	
Brandon McCormick - Brandon McCormick On Behalf of: Ginny Beigel, City of Vero Beach, 3; Lynne Mila, City of Clewiston, 4; Tom Reedy, Florida Municipal Power Pool, 6; - Brandon McCormick, Group Name FMPA	
Answer	No
Document Name	
Comment	
APPA does not agree with the scope of the CIP-012-1 R1 as it applies to Operational Planning Analysis, Real-time Assessment, and Real-time monitoring. Since Operational Planning Analysis data would not meet the 15-minute impact criteria used in the identification of BES Cyber Systems, this data would only be required to be protected as it is being transmitted between Control Centers. This inconsistency	

between the data systems identified by CIP-012-1 and those identified in other CIP standards may cause the unintended expansion of scope of the CIP Standards.

FMPA believes applying controls to the Operational Planning Analysis data may reduce the current ability of entities to share this data which may cause a reduction in BES reliability. Not all of this data goes from Control Center to Control Center but may go to (or from) a location outside of a Control Center and therefore would not be in scope of the drafted CIP-012 standard. APPA suggests removing the Operational Planning and Analysis data from the scope of this standard.

If the Operational Planning and Analysis data must be retained in the Standard, then APPA believes that an exemption for the communication of Operational Planning and Analysis data by email should be put in place. This would be similar to the exemption that exists for voice communication.

Likes 0	
Dislikes 0	

Response

Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino

Answer	No
Document Name	

Comment

We are concerned because unauthorized alteration of Operational Planning Analysis data does not pose a threat to the BES. This more appropriately addressed by TOP 010-1 reliability standard regarding the quality of the data. We note that Operational Planning Data is not real time data, as such we ask the STD to treat communicating Operational Planning Data Email exempt similar to the oral communication.

Likes 0	
Dislikes 0	
Response	
George Brown - Acciona Energy North America - 5	
Answer	No
Document Name	
Comment	

The requirement as written does not meet the criteria as outlined in the document titled "Ten Benchmarks of an Excellent Reliability Standard", benchmark 8. Clear Language. As the SDT stated in the rationale, the data in scope is the data as specified in TOP-003-3 and IRO-010-2. If this is in fact the case then the SDT should draw a clear and unambiguous line to these standards within the requirement. The addition of such language will also prevent unintentional scope reach.

Suggested language should be something to the following effect:

R1.2 The Responsible Entity, as applicable to its registered function, shall consider the data used for Operational Planning Analysis, Real-time Assessments, and Real-time monitoring to be the data as specified in:

- NERC Reliability Standard IRO-010-2, Requirement R1 and,
- NERC Reliability Standard TOP-003-3 — Operational Reliability Data, Requirement R1 and Requirement R2.

Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	

Answer	No
Document Name	
Comment	
Dominion asserts that data used for Operational Planning Analysis is often an ad-hoc report by exception (e.g., this line will be out or this unit will be de-rated) and because this data is often collected by a stand-alone system it can often be entered by several people within an organization and from several locations. Dominion is unclear on whether the entity expected to track which data is specifically entered from within a Control Center as opposed to from an office external to the Control Center. Many stand-alone systems are web-based and use https for all transactions. It is unclear what would qulaify as adequate evidence and that tracking locations and persons entering the information is not necessary.	
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	
Duke Energy has concerns about the decision to add Operational Planning Analysis information to the scope of the data protected by this standard. Currently, the scope of the CIP standards primarily focuses on real-time data, and bringing in Operational Planning Analysis pushes the scope of CIP standards to include Day Ahead. Also, in some instances, Operational Planning Analyses can be performed by a 3rd party or require data transmitted between entities via 3rd party tools. How would these affect be impacted by the applicability of the standard? Extending the CIP scope to apply to Day Ahead data is a departure, and could broaden the view of what tools (possibly including web-based tools?) could fall under CIP scope.	
Likes 0	

Dislikes 0	
Response	
RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC	
Answer	No
Document Name	
Comment	
If there is the need to scope sensitive BES data as it applies to Operational Planning Analysis, Real-time Assessment, and Real-time monitoring, it should all be scoped as data of the High Impact BES Cyber Systems.	
Likes 0	
Dislikes 0	
Response	
Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 3	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Lauren Price - American Transmission Company, LLC - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Greene - SERC Reliability Corporation - 10, Group Name SERC CIPC	
Answer	No
Document Name	3B-2016-02_CIP-012-1_Unofficial_Comment_Form_CIPC.docx
Comment	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1	
Answer	No
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Guy Andrews - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
We request clarification on the inclusion of data used for Operational Planning Analysis. This data does not have a 15 minute impact on the Bulk Electric System. This data is also typically exchanged between operations engineering staff who would not be considered to be a Control Center.	
Likes 0	
Dislikes 0	
Response	
Michael Shaw - Lower Colorado River Authority - 1, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	
Please provide guidance on whether or not email is in scope as a communication medium.	
Likes 0	
Dislikes 0	

Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
However, BPA questions the inclusion of Operational Planning Analysis.	
Likes 0	
Dislikes 0	
Response	
Sheranee Nedd - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	
RC, TOP and BA functional entities develop and disseminate specifications for the BES data they need to conduct Operational Planning Analysis, Real-time Assessment, and Real-time monitoring, in NERC '693' reliability standards TOP-003 and IRO-010. Relevant peer RCs/TOPs/BAs and others (GOs; GOPs; TOs; LSEs; DPs) are required by these standards to meet these data specifications. The scope of data subject to R1 is (or should be) thereby understood to be the data that entities both (i) specify in observance of these standards and (ii) transmit between the entity's and others' Control Centers.	
Likes 1	PSEG - PSEG Fossil LLC, 5, Kucey Tim
Dislikes 0	

Response	
Chris Scanlon - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon agrees that aligning with TOP-003-3 and IRO-010-2 is helpful for scoping CIP-012-1, and promotes consistent application of the NERC Standards.	
Likes 0	
Dislikes 0	
Response	
David Rivera - New York Power Authority - 3	
Answer	Yes
Document Name	
Comment	
No Comment	
Likes 0	
Dislikes 0	
Response	

Dermot Smyth - Con Ed - Consolidated Edison Co. of New York - 5, Group Name Con Edison	
Answer	Yes
Document Name	
Comment	
Same comment as question #1 above.	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
In the event mandatory standards are imposed, the scope should be limited to data that have well-defined terms.	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	

Comment	
TVA agrees that the entity needs to know what information is classified as BES sensitive data as it relates to operational planning analysis, real-time assessment, and real-time monitoring. In many cases some types of operational planning analysis data is housed in systems not classified as BES Cyber Systems and may not reside within an ESP.	
Likes 0	
Dislikes 0	
Response	
Janis Weddle - Public Utility District No. 1 of Chelan County - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb On Behalf of: Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 3, 5, 1, 6; James McBee, Great Plains Energy - Kansas City Power and Light Co., 3, 5, 1, 6; Jessica Tucker, Great Plains Energy - Kansas City Power and Light Co., 3, 5, 1, 6; Jim Flucke, Great Plains Energy - Kansas City Power and Light Co., 3, 5, 1, 6; - Douglas Webb	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Haley Sousa - Public Utility District No. 1 of Chelan County - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laurie Williams - PNM Resources - Public Service Company of New Mexico - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Puscas - ISO New England, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Con-Edison and Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Heather Morgan - EDP Renewables North America LLC - 5	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 3, Group Name FirstEnergy Corporation	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Shannon Fair - Colorado Springs Utilities - 1,3,5,6, Group Name Colorado Springs Utilities	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Frank Pace - Central Hudson Gas & Electric Corp. - 1	
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	
Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE does not have comments on this question.	
Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	
Document Name	
Comment	
The California ISO supports the comments of the Security Working Group (SWG).	
Likes 0	
Dislikes 0	
Response	

3. ***Implementation Plan: The SDT revised the Implementation Plan such that the standard and NERC Glossary terms are effective the first day of the first calendar quarter that is twelve (12) calendar months after the effective date of the applicable governmental authority's order approving the standard, or as otherwise provided for by the applicable governmental authority. Do you agree with this proposal? If you agree with the proposed implementation time period, please note the actions you will take that require this amount of time to complete. If you think an alternate implementation time period is needed – shorter or longer - please propose an alternate implementation plan and provide a detailed explanation of actions and time needed to meet the implementation deadline.***
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy

Answer	No
Document Name	
Comment	
Duke Energy disagrees with the proposed 12 month Implementation Plan. Certain aspects of achieving compliance with this standard (for example, implementing end to end encryption) would, in some instances, take a significant amount of time to put in place to due to the significance of the impact of these changes on critical systems. Further, applying these protections between Control Centers owned by more than one Responsible Entity will involve significant coordination, and additional time would be necessary to develop a shared understanding of existing technical limitations, develop agreements, and implement those new approaches for compliance. Duke Energy suggests that a phased implementation plan would be appropriate given the action necessary. We encourage the drafting team to consider an Implementation Plan of 12 months for R1. This would give time for the Responsible Entity to assess the Control Centers that are in its scope, decide on a method of protection, and involve any additional parties that may be necessary. We suggest a minimum of 24 months for the implementation date for R2 (implementing the plan developed in R1).	
Likes 0	
Dislikes 0	
Response	

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority

Answer	No
Document Name	
Comment	
TVA does not agree that twelve months is sufficient time to coordinate with other entities to agree on and implement protection mechanisms. Implementation may require coordination of plans across a large and/or diverse group of entities employing a variety of protective measures. TVA suggests 18-24 months would be a more realistic implementation period.	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	No
Document Name	
Comment	
Changes take time to evaluate and implement. The communication lines will have to be inventoried and evaluated. The data traveling across these lines will have to be inventoried and evaluated to ensure entities can evidence that they are protecting the itemized list of data included in the wording of R1 (Operational Planning Analysis, Real-time Assessment, and Real-time monitoring). Other activities that would need to occur for successful implementation would include preparation and delivery of guidance by regulatory bodies, communication and coordination with partner entities, configuration, and testing. At minimum, an 18-month implementation plan would be appropriate.	
Likes 0	
Dislikes 0	
Response	

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	
Comment	
Dominion asserts that budgets, resources, and other events between separate entities may require periods greater than 12 months. Dominion recommends that the implementation period be revised to 24 months.In addition, the time required to develop (R1), and then successfully implement (R2) would take longer than 12 months from the start date. 24 months should allow sufficient time to accomplish implementation of both requirements.	
Likes 0	
Dislikes 0	
Response	
George Brown - Acciona Energy North America - 5	
Answer	No
Document Name	
Comment	
This standard will require a collaborative effort between Control Centers of the various applicable Functional Entities to achieve the securities as required. As such, it may not feasible for some entities to implement these securities within 12 months. For example, a Reliability Coordinator (RC) Control Center will have contact with the Control Centers of several Balancing Authorities (BA), Generator Operators (GOP), Transmission Operators (TOP), Transmission Owners (TO) and other RCs. If a particular RC is unable to support the implementation of the securities as required in NERC CIP-012-1 then there will be a cascading and unnecessary non-compliance effect among the other Functional Entities that have Control Centers that transmit and receive this sensitive BES data with this particular RC's Control Center. A phase-in approach may be more appropriate for NERC CIP-012-1, based on schedules created using the Function Entity reliability hierarchy structure.	

Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino	
Answer	No
Document Name	
Comment	
For complex entities the identification and agreement on communication protocols and architecture may require extensive testing and learning. We recommend at least 18 months due to the quantity of details and logistics.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	
The IESO also encourages the drafting team to make the requirement forward-looking in regards to contracts currently in place. Provisions should be set for legacy contracts including grandfathering of existing agreements and equipment. Implementation of controls involving	

telecommunications providers will require coordination and scheduling to align to the providers' resource availability and reduce adverse impact on reliability. This should not require renewal and renegotiation of existing contracts until they reach the end of the existing contract period.

It should be noted that it is difficult to determine suitability of the implementation timeline when there are open questions about the viability of available solutions for adequate protections.

More time is necessary to allow for coordination with a large number of parties. This will require budgeting, planning, and scheduling with external resources for implementation. It will also require significant testing and validation by parties on both ends of a connection.

The IESO recommends a phased implementation with defined milestones similar to CIP-014. Consider the following:

- For creation of the plan, 12 months should be allowed to (1) conduct an impact assessments, (2) identify the approach to be included in the plan, (3) implementation milestones, and (4) implementation schedule. This could identify the communication links that have protections currently in place. The plan could also include identifying all links and protections requiring changes to address service contracts and related relationships to adjust for new protections. The plan could then be approved by an appropriate entity.
- For implementation of the plan, additional time should be allowed for budgeting, planning, and scheduling with external resources. This includes planning with other Responsible Entities as well as telecommunications providers.

Likes 2	Hydro One Networks, Inc., 1, Farahbakhsh Payam; Hydro One Networks, Inc., 3, Malozewski Paul
Dislikes 0	

Response

Brandon McCormick - Brandon McCormick On Behalf of: Ginny Beigel, City of Vero Beach, 3; Lynne Mila, City of Clewiston, 4; Tom Reedy, Florida Municipal Power Pool, 6; - Brandon McCormick, Group Name FMPA

Answer	No
Document Name	
Comment	

FMPA does not agree with the implementation proposal timeline. The time to implement R1 (develop a plan) should be 12 months from the time of the order.

Due to technical complexity, agreements (outsourced and between registered entities), procurement, contracts and coordination between registered entities (and provisioning of private networks), FMPA requests that the SDT consider the following options for R2 implementation:

- additional 24 months allowed to undertake implementation,
- using a phased implementation over a five or longer year period, or
- in recognition that there is the potential for several existing contracts will have to be replaced (and associated equipment) that affected contracts be grandfathered until new and or, replacements can be put in place.

Likes 0	
Dislikes 0	

Response

Frank Pace - Central Hudson Gas & Electric Corp. - 1

Answer	No
Document Name	

Comment

It would appear that the proposed implementation period is too short; however, it is difficult to determine if a demarcation point for compliance is not specified within the language of the Requirement.

Likes 0	
Dislikes 0	

Response

Donald Lock - Talen Generation, LLC - 5	
Answer	No
Document Name	
Comment	
The 12-month period provided in the implementation plan should be at least doubled. Developing a clear understanding of what is required could take some time, and to then scope the project, obtain bids and budget approval, receive materials and implement in whatever portion of the year remains may prove impractical.	
Likes 0	
Dislikes 0	
Response	
David Rivera - New York Power Authority - 3	
Answer	No
Document Name	
Comment	

1. The time to implement R1 (develop plan) could be 12 months from time of order. For implementation of R2 there should be an additional 24 months allowed to undertake implementation. This would include identifying all links and protections, with changes needed to address communications service contracts and related relationships to adjust for new protections. This would also involve inventory of data to comply with identification of all data transmitted between control centers.
2. Due to technical complexity, agreements (outsourced and between Entities), procurement, contracts and coordination between Entities (and provisioning of private networks), request that the SDT also consider the following option for R2 implementation:
    i. a phased implementation over a five or longer year period, or
    ii. to avoid impacting reliability, existing contracts, equipment, etc be grandfathered until new / replacements are in place.

Likes 0	
Dislikes 0	
Response	
Jennifer Hohenshilt - Talen Energy Marketing, LLC - 6	
Answer	No
Document Name	
Comment	
The 12-month period provided in the implementation plan should be at least doubled. Developing a clear understanding of what is required could take some time, and to then scope the project, obtain bids and budget approval, receive materials and implement in whatever portion of the year remains may prove impractical.	
Likes 0	
Dislikes 0	
Response	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	No
Document Name	
Comment	
The 12 month time period may only work for Entities who are vertically intergraded. The flow of applicable BES data within CIP-012-1 can be viewed as a “spider web” of data transfer for large RC foot-prints. With this being said, there may be non-compliance issues when one side of the data transference is protected and the other side is not. The SDT should propose a phased in approach to protecting data. A five (5) year implementation plan will allow entities to fund these projects. This is especially important to small entities. Per the NERC Guidance	

concerning “Phase Implementation Plans with Completion Percentages (http://www.nerc.com/pa/comp/guidance/CMEPPracticeGuidesDL/CMEP_Practice_Guide_Phased_Implementation_Completion_Percentages.pdf) please state that the CIP-012-1 does not fall under this guidance.	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	No
Document Name	
Comment	
See APPA Comments.	
Likes 0	
Dislikes 0	
Response	
James Poston - Santee Cooper - 3, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	

Recommend a 2 year Implementation Plan Period. For some entities, it may take a significant amount of time to agree on communication protocols and architecture with neighboring systems. Time is also needed to troubleshoot and test each connection point.	
Likes 0	
Dislikes 0	
Response	
Marty Hostler - Northern California Power Agency - 5	
Answer	No
Document Name	
Comment	
NCPA does not agree with the implementation proposal timeline. Due to technical complexity, agreements (outsourced and between REs), procurement, contracts and coordination between REs (and provisioning of private networks), NCPA requests that the SDT consider the following options for R2 implementation: • additional 24 months allowed to undertake implementation, • using a phased implementation over a five or longer year period, or • in recognition that there is the potential for several existing contracts will have to be replaced (and associated equipment) that affected contracts be grandfathered until new and or, replacements can be put in place.	
Likes 0	
Dislikes 0	
Response	

Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	
Comment	
NCPA does not agree with the implementation proposal timeline. Due to technical complexity, agreements (outsourced and between REs), procurement, contracts and coordination between REs (and provisioning of private networks), NCPA requests that the SDT consider the following options for R2 implementation: • additional 24 months allowed to undertake implementation, • using a phased implementation over a five or longer year period, or • in recognition that there is the potential for several existing contracts will have to be replaced (and associated equipment) that affected contracts be grandfathered until new and or, replacements can be put in place.	
Likes 0	
Dislikes 0	
Response	

Vivian Vo - APS - Arizona Public Service Co. - 3	
Answer	No
Document Name	
Comment	
The proposed implementation plan does not consider complexities associated with implementing technical solutions reliant on inter-entity coordination and agreement. The proposed implementation plan does not recognize the prerequisite of mutual agreement between entities regarding a compatible technical solution or the time necessary to complete such prerequisite. Moreover, it does not appear to contemplate	

a potential need for dispute resolution when a transmitting entity and receiving entity cannot agree on a solution. Finally, any implementation, testing, etc. can only occur once the mutually agreed-upon solution has been identified, budgeted, and procured. For these reasons, AZPS proposes extending the implementation plan to at least twenty-four (24) calendar months. Two years would likely allot adequate time to identify, agree upon, and procure appropriate technical solutions in coordination with other entities.	
Likes 0	
Dislikes 0	
Response	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	No
Document Name	
Comment	
The Implementation Plan should be modified to allow 24 months for the implementation phase (R2) due to the potential impact resulting from the necessity of redesigning communications architectures for secure communications between Control Centers.	
Likes 0	
Dislikes 0	
Response	
Heather Morgan - EDP Renewables North America LLC - 5	
Answer	No
Document Name	
Comment	

Generator Operator Control Centers are required to follow specifications pursuant to the requirements outlined by RCs, ISO,s RTOs, BAs, and TOPs. To ensure GOP's are able to properly carry out requirements for all of these parties and CIP-012-2, CIP-012-2's Implementation Plan should be phased in similar to IRO-010, and TOP-003. Otherwise, GOP Control Centers will not be able to properly plan for any requirements delivered by the interconnecting authorities as a result of this Standard.	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	No
Document Name	
Comment	
Request changing 12 months to 18 months in the implentation plan to allow time to make any required changes including design, procurement, CIP assesment and deployment.	
Likes 0	
Dislikes 0	
Response	
Aaron Austin - AEP - 3	
Answer	No
Document Name	
Comment	

AEP suggests that the implementation time frame should be extended to at least 24 months to allow for activities such as coordination, budgeting, procurement, implementation and testing.	
Likes 0	
Dislikes 0	
Response	
Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	No
Document Name	
Comment	
NRECA asserts that smaller entities may need to procure equipment and implement technical controls that are not currently in place. The implementation of the plan(s) detailed in requirement R1 could be impacted by budget cycles, procurement processes, and third party vendor availability. NRECA recommends that the implementation plan be revised to allow 12 months for the development of the plan in requirement R1 and 24 months for the implementation.	
Likes 0	
Dislikes 0	
Response	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	No
Document Name	
Comment	

Hydro Québec is in agreement with TFIST's comments below in regards to taking into consideration technical complexities and coordination between entities; however we suggest that the documented plan in R1 include an implementation plan with deadlines not exceeding 36 months, rather than a prescribed delay for implementing R2. Furthermore, clarifications are requested in regards to the question"please note the actions you will take that require this amount of time to complete.

1. The time to implement R1 (develop plan) could be 12 months from time of order. For implementation of R2 there should be an additional 24 months allowed to undertake implementation. This would include identifying all links and protections, with changes needed to address communications service contracts and related relationships to adjust for new protections. This would also involve inventory of data to comply with identification of all data transmitted between control centers.

2. Due to technical complexity, agreements (outsourced and between Entities), procurement, contracts and coordination between Entities (and provisioning of private networks), request that the SDT consider:

a)a phased implementation over a five or longer year period, or b) to avoid impacting reliability, that existing contracts, equipment, etc stay in place. New contracts / equipment will need to follow this new Standard.

Likes 0	
Dislikes 0	
Response	
Lona Calderon - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	

SRP requests 24 calendar months due to the complex details and logistics associated with implementation. The Impact from encryption is unknown. Because the data is being sent in real-time, it is difficult to test how encryption will affect reliability.

More research and evaluation is required to understand the implications encryption will have as it may require architecture changes to account for the extra computing resources required. Additionally, time is required to budget for funds in order to support any required infrastructure improvements required.	
Likes 0	
Dislikes 0	
Response	
Thomas Breene - WEC Energy Group, Inc. - 3	
Answer	No
Document Name	
Comment	
The 12 month time period may only work for Entities who are vertically intergraded. The flow of applicable BES data within CIP-012-1 can be viewed as a "spider web" of data transfer for large RC foot-prints. With this being said, there may be non-compliance issues when one side of the data transference is protected and the other side is not. The SDT should propose a phased in approach to protecting data. A five (5) year implementation plan will allow entities to fund these projects. This is especially import to small entities. Per the NERC Guidance concerning "Phase Implementation Plans with Completion Percentages (http://www.nerc.com/pa/comp/guidance/CMEPPracticeGuidesDL/CMEP_Practice_Guide_Phased_Implementation_Completion_Percentages.pdf) please state that the CIP-012-1 does not fall under this guidance.	
Likes 0	
Dislikes 0	
Response	
Russell Noble - Cowlitz County PUD - 3	
Answer	No

Document Name	
Comment	
Cowlitz PUD supports the comments submitted by APPA.	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	No
Document Name	
Comment	
We recommend at least 18 months due to the quantity of details and logistics.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Con-Edison and Dominion	
Answer	No
Document Name	
Comment	

· The time to implement R1 (develop plan) could be 12 months from time of order. For implementation of R2 there should be an additional 24 months allowed to undertake implementation. This would include identifying all links and protections, with changes needed to address communications service contracts and related relationships to adjust for new protections. This would also involve inventory of data to comply with identification of all data transmitted between control centers.

· Due to technical complexity, agreements (outsourced and between Entities), procurement, contracts and coordination between Entities (and provisioning of private networks), request that the SDT also consider the following option for R2 implementation:

a. a phased implementation over a five or longer year period, or

b. to avoid impacting reliability, existing contracts, equipment, etc. be grandfathered until new / replacements are in place.

Likes 0	
Dislikes 0	
Response	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	

ERCOT ISO signs on to the ITC SWG comments:

The ITC SWG also encourages the drafting team to make the requirement forward-looking in regards to contracts currently in place. Provisions should be set for legacy contracts including grandfathering of existing agreements and equipment. Implementation of controls involving telecommunications providers will require coordination and scheduling to align to the providers' resource availability and reduce adverse impact on reliability. This should not require renewal and renegotiation of existing contracts until they reach the end of the existing contract period.

It should be noted that it is difficult to determine suitability of the implementation timeline when there are open questions about the viability of available solutions for adequate protections.

More time is necessary to allow for coordination with a large number of parties. This will require budgeting, planning, and scheduling with external resources for implementation. It will also require significant testing and validation by parties on both ends of a connection.

The ITC SWG recommends a phased implementation with defined milestones similar to CIP-014. Consider the following:

- For creation of the plan, 12 months should be allowed to (1) conduct an impact assessments, (2) identify the approach to be included in the plan, (3) implementation milestones, and (4) implementation schedule. This could identify the communication links that have protections currently in place. The plan could also include identifying all links and protections requiring changes to address service contracts and related relationships to adjust for new protections. The plan could then be approved by an appropriate entity.
- For implementation of the plan, additional time should be allowed for budgeting, planning, and scheduling with external resources. This includes planning with other Responsible Entities as well as telecommunications providers.

Likes 0	
Dislikes 0	

Response

Shelby Wade - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company

Answer	No
Document Name	

Comment

We support SERC's comments.

Likes 0	

Dislikes 0	
Response	
Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 3	
Answer	No
Document Name	
Comment	
Tacoma Power supports the comments of APPA	
Likes 0	
Dislikes 0	
Response	
Theresa Rakowsky - Puget Sound Energy, Inc. - 1	
Answer	No
Document Name	
Comment	
PSE believes a 24 month implementation period and/or phased implementation approach is appropriate due to required coordination between registered entities, potential need for renegotiation of contracts and/or agreements with other entities, and potential for significant technical complexity for implementation.	
Likes 0	
Dislikes 0	
Response	

Jack Cashin - American Public Power Association - 4	
Answer	No
Document Name	
Comment	
APPA does not agree with the implementation proposal timeline. The time to implement R1 (develop a plan) should be 12 months from the time of the order. Due to technical complexity, agreements (outsourced and between registered entities), procurement, contracts and coordination between registered entities (and provisioning of private networks), APPA requests that the SDT consider the following options for R2 implementation: • additional 24 months allowed to undertake implementation, • using a phased implementation over a five or longer year period • in recognition that there is the potential for several existing contracts will have to be replaced (and associated equipment) that affected contracts be grandfathered until new and or, replacements can be put in place.	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	

CenterPoint Energy recommends the effective date for CIP-012-1 to be 24 months after FERC approval. For instances where applicable data is being transmitted between Control Centers owned by two or more separate Responsible Entities, additional time is needed to coordinate plans and develop agreements to ensure adequate protection is applied.	
Likes 0	
Dislikes 0	
Response	
Warren Cross - ACES Power Marketing - 1,3,4,5 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standards Collaborators	
Answer	No
Document Name	
Comment	
New entities that are impacted by the new definition should be treated as “newly identified CIP facilities” and should be given the standard 18 month implementation period. Not the proposed 12 month implementation period. Budgetary cycles would need to be considered and an additional reason for the 18 months.	
Likes 0	
Dislikes 0	
Response	
Sheranee Nedd - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	No
Document Name	
Comment	

PSEG Supports the NPCC comments.	
Likes 1	PSEG - PSEG Fossil LLC, 5, Kucey Tim
Dislikes 0	
Response	
Michael Puscas - ISO New England, Inc. - 2	
Answer	No
Document Name	
Comment	
The time to implement the first requirement (develop plan) could be 12 months from time of order. For implementation of the plan, however (R2) there should be an additional 12 months allowed to undertake implementation. This would include identifying all links and protections, with changes needed to address communications service contracts and related relationships to adjust for new protections.	
Likes 0	
Dislikes 0	
Response	
David Greyerbiehl - CMS Energy - Consumers Energy Company - 5	
Answer	No
Document Name	
Comment	
Twelve calendar months for implementation may not be sufficient, twenty-four calendar months should be recommended.	

Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
BPA requests clarification about what “Physically protecting the communication links transmitting the data” in section 1.1 means. If it means protecting the data at the source (at the Control Center), the implementation period is acceptable. BPA will be required to update customer agreements during the implementation period. If it means the data must be protected throughout the transmission, it would seem that could only be accomplished with encryption. For cases where the existing equipment is not capable of encryption, BPA cannot propose an implementation timeline or solution other than technically feasible exception.	
Likes 0	
Dislikes 0	
Response	
James Anderson - CMS Energy - Consumers Energy Company - 1	
Answer	No
Document Name	
Comment	

Twelve calendar months for implementation may not be sufficient, twenty-four calendar months should be recommended.	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	No
Document Name	
Comment	
Utility Services does not agree with the implementation proposal timeline. The time to implement R1 (develop a plan) should be 12 months from the time of the order. Due to technical complexity, agreements (outsourced and between registered entities), procurement, contracts and coordination between registered entities (and provisioning of private networks), UTILITY SERVICES requests that the SDT consider the following options for R2 implementation: · additional 24 months allowed to undertake implementation, · using a phased implementation over a five or longer year period, or · in recognition that there is the potential for several existing contracts will have to be replaced (and associated equipment) that affected contracts be grandfathered until new and or, replacements can be put in place.	
Likes 0	
Dislikes 0	
Response	

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No
Document Name	
Comment	
Southern Company feels that 12 months is not enough time to implement the Standard as currently written. Implementation of the proposed methods of compliance could embark entities on budget and procurement processes to acquire new, upgraded, or revamped hardware, software, or other physical components at existing sites, and this can be a lengthy process. Southern recommends at least a 24 month or greater implementation timeframe. Southern agrees with comments provided by other commenters that the complexity of the technology solutions to be implemented, the number of interconnecting lines to secure, connection point testing, and coordination requirements with external stakeholders are additional factors supporting a 2 year implementation period.	
Likes 0	
Dislikes 0	
Response	
Ronald Donahey - TECO - Tampa Electric Co. - 3	
Answer	No
Document Name	
Comment	
If additional contracts/agreements are required to address a plan for other entities, Registered Entities may need a longer time to implement the plan (Requirement R2). Tampa Electric Company recommends an 18 month timeframe for Requirement 2.	
Likes 0	
Dislikes 0	

Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	No
Document Name	
Comment	
The Standard Review Group has a concern that all Implementation needs may not be met in a timely fashion at the twelve (12) calendar month time frame. We would recommend that the drafting team extends the deadline to eighteen (18) calendar months. Due to technological changes needed to secure the data and collaboration between sending and receiving party, we feel more time is needed to implement the standard.	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 5	
Answer	No
Document Name	
Comment	
Eighteen calendar months after the approval of the control center definition and the CIP-012-1 standard to allow entities time to evaluate the impact of the changes effected by the new standard and implement an appropriate response.	
Likes 0	
Dislikes 0	

Response	
James Gower - Entergy - NA - Not Applicable - SERC	
Answer	No
Document Name	
Comment	
Cannot support at this time until additional clarity is given to requirements for written communications outside of operational data and for Operational Planning Analysis data. If corporate systems require protection that could greatly affect implementation timelines. Additionally, the twelve month window may fall outside of yearly budget planning, compressing project planning timelines.	
Likes 0	
Dislikes 0	
Response	
Mark Riley - Associated Electric Cooperative, Inc. - 1	
Answer	No
Document Name	
Comment	
AECI asserts that smaller entities may need to procure equipment and implement technical controls that are not currently in place. The implementation of the plan(s) detailed in requirement R1 could be impacted by budget cycles, procurement processes, and third party vendor availability. AECI recommends that the implementation plan be revised to allow 12 months for the development of the plan in requirement R1 and 24 months for the implementation	
Likes 0	

Dislikes 0	
Response	
Guy Andrews - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	
• Additional time would be required to plan, budget, and implement this Standard. Further, only allowing 12 months for implementation may limit the technology solutions that may be implemented to only those that can be accomplished with minimal planning and testing. GSOC requests twenty-four months.	
Likes 0	
Dislikes 0	
Response	
Annette Johnston - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	No
Document Name	
Comment	
At least three years is needed in order to coordinate with other entities, including specification, design, budgeting, implementation and testing.	
Likes 0	
Dislikes 0	

Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	
Comment	
See MidAmerican Energy Company comments.	
Likes 0	
Dislikes 0	
Response	
Haley Sousa - Public Utility District No. 1 of Chelan County - 5	
Answer	No
Document Name	
Comment	
The coordination time required to perform a migration to secure communications protocols is expected to take longer than the schedule presented by the SDT. CHPD recommends at least twenty-four (24) calendar months to implement communication updates and implement other available protection measures.	
Likes 0	
Dislikes 0	
Response	

Janis Weddle - Public Utility District No. 1 of Chelan County - 6	
Answer	No
Document Name	
Comment	
The coordination time required to perform a migration to secure communications protocols is expected to take longer than the schedule presented by the SDT. CHPD recommends at least twenty-four (24) calendar months to implement communication updates and implement other available protection measures.	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Greene - SERC Reliability Corporation - 10, Group Name SERC CIPC	
Answer	No
Document Name	3B-2016-02_CIP-012-1_Unofficial_Comment_Form_CIPC.docx

Comment	
Likes 0	
Dislikes 0	
Response	
Lauren Price - American Transmission Company, LLC - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
A region-wide agreement may be difficult to develop and execute in a year. Tri-State believes 18 months would be more appropriate.	
Likes 0	
Dislikes 0	

Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE	
Answer	Yes
Document Name	
Comment	
Xcel Energy believes that the Implementation Plan would allow sufficient time for our operating companies to implement required controls specified in the language of CIP-012-1. However, Xcel Energy would require coordination from up to 25 other Responsible Entities is communicates BES data with and cannot speak to their abilities. Any agreements in coordination between entities would need to go through a legal review process, which could take more than 12 months to formalize and implement. A 24 month implementation period may be more feasible given the legal review challenges that would inevitably occur.	
Likes 0	
Dislikes 0	
Response	
David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
OPG has some concerns and recommends a graded approach implementation over a longer period of time. The communications links requiring protections will require inventory; this will be a complex task for the RC.	

The recommended 12 months may be sufficient for the inventory, however we also need to determine the applicable solution and agree on the solution with another entities.	
Likes 0	
Dislikes 0	
Response	
Laura McLeod - NB Power Corporation - 5	
Answer	Yes
Document Name	
Comment	
See 1 above. Note that additional time may be required to reach consensus between entities when establishing security protocols.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb On Behalf of: Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 3, 5, 1, 6; James McBee, Great Plains Energy - Kansas City Power and Light Co., 3, 5, 1, 6; Jessica Tucker, Great Plains Energy - Kansas City Power and Light Co., 3, 5, 1, 6; Jim Flucke, Great Plains Energy - Kansas City Power and Light Co., 3, 5, 1, 6; - Douglas Webb	
Answer	Yes
Document Name	
Comment	

The company will review current systems and protections to identify if further action is required to protect the communications links between control centers as set forth in the approved Standard.	
Likes 0	
Dislikes 0	
Response	
RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Dermot Smyth - Con Ed - Consolidated Edison Co. of New York - 5, Group Name Con Edison	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Philip Huff - Arkansas Electric Cooperative Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Shannon Fair - Colorado Springs Utilities - 1,3,5,6, Group Name Colorado Springs Utilities	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Alice Wright - Arkansas Electric Cooperative Corporation - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Michael Shaw - Lower Colorado River Authority - 1, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laurie Williams - PNM Resources - Public Service Company of New Mexico - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 3	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	
Document Name	
Comment	
The California ISO supports the comments of the Security Working Group (SWG).	
Likes 0	
Dislikes 0	
Response	
Kristine Ward - Seminole Electric Cooperative, Inc. - 1,2,4,5,6 - FRCC	
Answer	
Document Name	
Comment	
SECI would like examples of evidence so we know how to proceed	
Likes 0	
Dislikes 0	

Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	

This question implies there are NERC Glossary terms in the Implementation Plan. There are no NERC Glossary terms in the CIP-012-1 Implementation Plan.

Texas RE does not oppose the enforcement timelines set forth in the proposed Implementation Plan. However, Texas RE respectfully requests that the SDT provide a specific justification for any proposed implementation timeframes, as well as any revisions to the timeframes as currently proposed. The goal is to ensure there are no issues with the implementation plan such as not having an initial performance date where one is needed or not including information for new facilities such as the instance that led to an errata change in the PRC-023-4 implementation plan. These issues cause confusion and ambiguity for both registered entities and Regional Entities upon enforcement of the standard.

Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 3, Group Name FirstEnergy Corporation	
Answer	
Document Name	
Comment	

FirstEnergy recommends adjusting the Implementation Plan time period to become effective the first day of the first calendar quarter that is eighteen (18) calendar months after the effective date of the applicable governmental authority's order approving the standard. The additional time will be needed to ensure that the implementation of any new technology (e.g. encryption) does not impact reliability of the BES.

Likes 0	
Dislikes 0	
Response	

4. *The SDT believes proposed CIP-012-1 provides entities with flexibility to meet the reliability objectives in a cost effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost effective approaches, please provide your recommendation and, if appropriate, technical justification.*

Janis Weddle - Public Utility District No. 1 of Chelan County - 6	
Answer	No
Document Name	
Comment	
CHPD cannot determine if the objectives may be accomplished in a cost-effective manner until further clarification is provided for physical or other equally effective protection measures and the request for electronic mail exclusion is added. CHPD also has concerns with vendor availability, with respect to the system software implementation that will be required for all entities industry-wide. The comments provided by other entities to develop an industry-wide encryption specification is appealing and CHPD believes that would provide a better method for achieving the desired intra-entity security.	
Likes 0	
Dislikes 0	
Response	

Haley Sousa - Public Utility District No. 1 of Chelan County - 5	
Answer	No
Document Name	
Comment	
CHPD cannot determine if the objectives may be accomplished in a cost-effective manner until further clarification is provided for physical or other equally effective protection measures and the request for electronic mail exclusion is added. CHPD also has concerns	

with vendor availability, with respect to the system software implementation that will be required for all entities industry-wide. The comments provided by other entities to develop an industry-wide encryption specification is appealing and CHPD believes that would provide a better method for achieving the desired intra-entity security.	
Likes 0	
Dislikes 0	
Response	
Laura McLeod - NB Power Corporation - 5	
Answer	No
Document Name	
Comment	
See 2 above.	
Likes 0	
Dislikes 0	
Response	
James Gower - Entergy - NA - Not Applicable - SERC	
Answer	No
Document Name	
Comment	

Cannot agree with the flexibility and cost effectiveness until additional clarity is given to requirements for written communications outside of operational data and Operational Planning Analysis. If corporate systems require protection that could greatly affect potential cost.	
Likes 0	
Dislikes 0	
Response	
Ronald Donahey - TECO - Tampa Electric Co. - 3	
Answer	No
Document Name	
Comment	
Until industry is able to determine the extent of information to be protected extends beyond the real-time 15 minute time frame, we are not able to agree with the statement regarding cost-effective manner.	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No
Document Name	
Comment	

The cost of implementing the intended protections, as they are understood by Southern, will be prohibitive. See the response to Question 1 as the primary driver for our disagreement with this question, as well as other supporting information provided in response to Question 3.	
Likes 0	
Dislikes 0	
Response	
James Anderson - CMS Energy - Consumers Energy Company - 1	
Answer	No
Document Name	
Comment	
More flexibility and less guidance could lead to inconsistency on requirement implementation among different entities.	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	

If it means the data must be protected throughout the transmission, it would seem that could only be accomplished with encryption. For cases where the existing equipment is not capable of encryption, replacement will be costly and implementation lengthy.	
Likes 0	
Dislikes 0	
Response	
David Greyerbiehl - CMS Energy - Consumers Energy Company - 5	
Answer	No
Document Name	
Comment	
More flexibiity and less guidance could lead to inconsistency on requirement implentation among different entities.	
Likes 0	
Dislikes 0	
Response	
Michael Puscas - ISO New England, Inc. - 2	
Answer	No
Document Name	
Comment	
To fully assess the logistics and costs associated with compliance, some guidance or specification of boundaries of communications links involved would be required for entities to complete assessment of impacts to their operations.	

Likes 0	
Dislikes 0	
Response	
Warren Cross - ACES Power Marketing - 1,3,4,5 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standards Collaborators	
Answer	No
Document Name	
Comment	
(1) The standard doesn't directly address the Inter-Control Center Communications Protocol (ICCP) for exchanging data between control centers or utilities. Will those ICCP servers and supportive infrastructure need to be upgraded or replaced with data encryption capabilities to support compliance with this standard? (2) The standard doesn't provide any direction as to what is the level of physical and logical protection that is mandatory. We ask the SDT to develop guidance to clarify this ambiguity and identify how all entities can achieve a minimum level of compliance.	
Likes 0	
Dislikes 0	
Response	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
ERCOT ISO signs on to the ITC SWG comments:	

In addition to the comments provided in response to question 3, the SWG offers these comments regarding cost effectiveness. Open Source options to satisfy the requirement to protect communication links and sensitive bulk electric system data communicated between bulk electric systems Control Centers are limited. Few options generally translated to high vendor leverage, which could lead to high implementation costs. It is unclear how or whether costs could be shared among participants in the network. Architectural changes to support these requirements should be spread out over several years. Plus there will be business impacts.	
Likes 0	
Dislikes 0	
Response	
Lona Calderon - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
SRP needs more detail on what would be acceptable as physical security to determine if the standard provides adequate flexibility. Also, as stated in response to question 3, significant capital may need to be budgeted in order to implement architecture improvements to address the required computing resources for encrypting and decrypting of data. Additionally, SRP agrees with LPPC's comment that an industry-wide initiative for an encryption specification may be a more cost-effective approach than a new standard.	
Likes 0	
Dislikes 0	
Response	
Aaron Austin - AEP - 3	
Answer	No

Document Name	
Comment	
AEP believes that most entities are at the mercy of what Balancing Authorities and Reliability Coordinators will require. This coupled with the fact that data for Operational Planning and Analysis is included, flexibility may lead to variability and as such makes it only a presumption that solutions will be cost effective.	
Likes 0	
Dislikes 0	
Response	
Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	
Comment	
NCPA does not agree that the standard provides entities with the flexibility to implement the standard cost-effectively and offers these further suggestions. To fully assess the logistics and costs associated with compliance, some guidance or specification of boundaries of communications links involved would be required for entities to complete assessment of impacts to their operations. In addition, architectural changes should be spread out over several budget cycles (years).	
Likes 0	
Dislikes 0	
Response	
Marty Hostler - Northern California Power Agency - 5	

Answer	No
Document Name	
Comment	
NCPA does not agree that the standard provides entities with the flexibility to implement the standard cost-effectively and offers these further suggestions. To fully assess the logistics and costs associated with compliance, some guidance or specification of boundaries of communications links involved would be required for entities to complete assessment of impacts to their operations. In addition, architectural changes should be spread out over several budget cycles (years).	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	No
Document Name	
Comment	
See APPA Comments.	
Likes 0	
Dislikes 0	
Response	
Alice Wright - Arkansas Electric Cooperative Corporation - 4	
Answer	No

Document Name	
Comment	
See attachment	
Likes 0	
Dislikes 0	
Response	
Philip Huff - Arkansas Electric Cooperative Corporation - 3	
Answer	No
Document Name	
Comment	
Please see our comments to Question 1. The additional flexibility in this context has the potential to cause more confusion when selecting a mechanisms to secure the data.	
Likes 0	
Dislikes 0	
Response	
David Rivera - New York Power Authority - 3	
Answer	No
Document Name	
Comment	

1. To fully assess the logistics and costs associated with compliance, some guidance or specification of boundaries of communications links involved would be required for entities to complete assessment of impacts to their operations.
2. Architectural changes should be spread out over several budget cycles (years). Plus there will be business impacts. See comments to Q3

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	No
Document Name	

Comment

In addition to the comments provided in response to question 3, the IESO offers these comments regarding cost effectiveness. Open Source options to satisfy the requirement to protect communication links and sensitive bulk electric system data communicated between bulk electric systems Control Centers are limited. Few options generally translated to high vendor leverage, which could lead to high implementation costs. It is unclear how or whether costs could be shared among participants in the network. Architectural changes to support these requirements should be spread out over several years. Plus there will be business impacts.

Likes 2	Hydro One Networks, Inc., 1, Farahbakhsh Payam; Hydro One Networks, Inc., 3, Malozewski Paul
Dislikes 0	

Response

Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith,

Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino	
Answer	No
Document Name	
Comment	
It may be more cost effective if an industry wide initiative is conducted with encryption specifications.	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	No
Document Name	
Comment	
There will likely be additional costs associated with administrative overhead, hardware, and software, as well as costs associated with monitoring the performance of the implemented solutions.	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	No

Document Name	
Comment	
TVA suggests additional guidance is needed to identify examples of acceptable standard security mechanisms for exchanging data between entities. Without clearer guidance some entities may out of an abundance of caution spend beyond what is necessary to mitigate this risk, or expend unnecessary effort determining a mutual security mechanism.	
Likes 0	
Dislikes 0	
Response	
Lauren Price - American Transmission Company, LLC - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	Yes
Document Name	
Comment	

See MidAmerican Energy Company comments.	
Likes 0	
Dislikes 0	
Response	
Annette Johnston - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	Yes
Document Name	
Comment	
The three bullets are constructive.	
Likes 0	
Dislikes 0	
Response	
Guy Andrews - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
no comments	
Likes 0	

Dislikes 0	
Response	
David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
OPG recommends further collaboration to further enhance the cost effectiveness. Solution implementation will require collaboration when the communication link is between CC belonging to different entities. There is also the issue of agreed solution; for example the stronger the protection implemented the higher the budgetary costs. If this may not be an issue for the RC it can be an issue for a small entity required to report to the RC via these communication links.	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Utility Services agrees that the standard provides entities with the flexibility to implement the standard cost-effectively and offers these further suggestions. To fully assess the logistics and costs associated with compliance, some guidance or specification of boundaries of communications links involved would be required for entities to complete assessment of impacts to their operations. In addition, architectural changes should be spread out over several budget cycles (years).	

Likes 0	
Dislikes 0	
Response	
Sheranee Nedd - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	
PSEG supports the NPCC comments.	
Likes 1	PSEG - PSEG Fossil LLC, 5, Kucey Tim
Dislikes 0	
Response	
Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 3	
Answer	Yes
Document Name	
Comment	
Tacoma Power supports the comments of APPA	
Likes 0	
Dislikes 0	
Response	

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Con-Edison and Dominion	
Answer	Yes
Document Name	
Comment	
· To fully assess the logistics and costs associated with compliance, some guidance or specification of boundaries of communications links involved would be required for entities to complete assessment of impacts to their operations. · Architectural changes should be spread out over several budget cycles (years), and there will be business impacts. See comments to Q3	
Likes 0	
Dislikes 0	
Response	
Russell Noble - Cowlitz County PUD - 3	
Answer	Yes
Document Name	
Comment	
Cowlitz PUD supports the comments submitted by APPA.	
Likes 0	
Dislikes 0	
Response	

Thomas Breene - WEC Energy Group, Inc. - 3	
Answer	Yes
Document Name	
Comment	
Thank you for adding the third bullet of R1.	
Likes 0	
Dislikes 0	
Response	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	Yes
Document Name	
Comment	
1. To fully assess the logistics and costs associated with compliance, some guidance or specification of boundaries of communications links involved would be required for entities to complete assessment of impacts to their operations. 2. Architectural changes should be spread out over several budget cycles (years). Plus there will be business impacts. See comments to Q3.	
Likes 0	
Dislikes 0	
Response	

Heather Morgan - EDP Renewables North America LLC - 5	
Answer	Yes
Document Name	
Comment	
None at this time	
Likes 0	
Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 3	
Answer	Yes
Document Name	
Comment	
While the Standard is sufficiently flexible for an individual responsible entity, it leaves a potential chasm between different entities' interpretation of cost-effective approaches. A top-tier utility's impression of a cost effective approach may not match a smaller neighbor's idea of a cost effective approach. Such a disparity could encumber both large and small entities with disparate concerns that complicate negotiation and agreement on appropriate solutions.	
Likes 0	
Dislikes 0	
Response	

Chris Scanlon - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon agrees with the approach used in CIP-012-1, which allows each Registered Entity to analyze risk and use discretion in determining the best risk mitigation implementation for protecting transmission of applicable data.	
Likes 0	
Dislikes 0	
Response	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
Thank you for adding the third bullet of R1	
Likes 0	
Dislikes 0	
Response	
Dermot Smyth - Con Ed - Consolidated Edison Co. of New York - 5, Group Name Con Edison	
Answer	Yes

Document Name	
Comment	
To fully assess the logistics and costs associated with compliance, some guidance or specification of boundaries of communications links involved should be provided so that entities can perform an assessment of impacts to their operations.	
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 agrees that the language provided in R1 appears to provide a Responsible Entity flexibility in how it may implement the standard, but concern exists in the amount of protection options given. Additional documentation such as Implementation Guidance including additional suggestions for implementation may give entities more options to consider, while still keeping the flexibility of determining what is the most suitable method of protection for said entity.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb On Behalf of: Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 3, 5, 1, 6; James McBee, Great Plains Energy - Kansas City Power and Light Co., 3, 5, 1, 6; Jessica Tucker, Great Plains Energy - Kansas City Power and Light Co., 3, 5, 1, 6; Jim Flucke, Great Plains Energy - Kansas City Power and Light Co., 3, 5, 1, 6; - Douglas Webb	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laurie Williams - PNM Resources - Public Service Company of New Mexico - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Shaw - Lower Colorado River Authority - 1, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Greene - SERC Reliability Corporation - 10, Group Name SERC CIPC	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Theresa Rakowsky - Puget Sound Energy, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
sean erickson - Western Area Power Administration - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Shelby Wade - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 3, Group Name FirstEnergy Corporation	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Poston - Santee Cooper - 3, Group Name Santee Cooper	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Shannon Fair - Colorado Springs Utilities - 1,3,5,6, Group Name Colorado Springs Utilities	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Hohenshilt - Talen Energy Marketing, LLC - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Donald Lock - Talen Generation, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Frank Pace - Central Hudson Gas & Electric Corp. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
George Brown - Acciona Energy North America - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Nicholas Lauriat - Network and Security Technologies - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jack Cashin - American Public Power Association - 4	
Answer	
Document Name	
Comment	

APPA agrees that the standard provides entities with the flexibility to implement the standard cost-effectively and offers these further suggestions. To fully assess the logistics and costs associated with compliance, some guidance or specification of boundaries of communications links involved would be required for entities to complete assessment of impacts to their operations. In addition, architectural changes should be spread out over several budget cycles (years).	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE does not have comments on this questions.	
Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	
Document Name	
Comment	

The California ISO supports the comments of the Security Working Group (SWG).	
Likes 0	
Dislikes 0	
Response	

5. ***If you have additional comments on the proposed CIP-012-1 – Cyber Security -- Communication Networks drafted in response to the FERC directive that you have not provided in response to the questions above, please provide them here.***

Richard Vine - California ISO - 2	
Answer	
Document Name	
Comment	
The California ISO supports the comments of the Security Working Group (SWG).	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	
Document Name	
Comment	
TVA notes that the requirement language focuses on the risk of unauthorized disclosure or modification of data. In an operational environment the integrity and availability legs of the CIA triad are more critical than the confidentiality. TVA suggests consider revising to focus on ensuring the integrity and availability of the data.	
Likes 0	
Dislikes 0	

Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	
Document Name	
Comment	

Applicability:

Based on the first 2 questions in the proposed RSAW requiring entities to prove that the standard does not apply to them, could the Applicability section of the standard be modified to indicate that the standard only applies to those specific registered entities (e.g., GOPs and TOs) that maintain Control Centers AND transmit data between Control Centers?

Additionally, the proposed standard does not provide a sufficient level of detail on how entities should work together to handle security concerns across a communication network. The standard should clearly identify where the obligations for protecting data in a communication network start and end per entity.

Technical Rationale:

Does the TO field asset box on page # 5 of Technical Rationale and Justification for CIP-012-1 document include TO Control Centers? If no, where are TO Control Centers represented ?

Implementation Guidance:

CIP-012 R2 requires the Responsible Entity to implement on or more documented plan(s) to mitigate the risk of the unauthorized disclosure or modification of applicable data whish being transmitted between Control Centers. Without implementation guidance describing how to accomplish this risk mitigation either physically protecting the communication links transmitting the data or logically protecting the data during transmission; or some other equally effective means it is difficult to predict the amount of time that would be required to implement this requirement part and therefore we cannot assume the 12 months prescribed in the proposed implementation plan is adequate.

Likes 0	
Dislikes 0	
Response	
Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	
Document Name	
Comment	
If the region is responsible for the system, what does the entity have to do for compliance? All entities would have to coordinate with the region on a solution. The solution may require additional equipment to be installed. A region-wide formal agreement may be difficult to develop and execute in a year.	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	
Document Name	
Comment	
Even though ReliabilityFirst votes in the affirmative, ReliabilityFirst provides the following comments for consideration: 1. Requirement R2	

i. Requirement R2 of the Standard does not identify a "reasonable" timeline for implementing the plan identified in R1. This lack of time determinant could lead to prolonged and needless delay in implementing the required protections.

ii. Requirement R2 uses the phrase "CIP Exceptional Circumstances". The intent is "to protect confidentiality and integrity of data transmitted between Control Centers required for reliable operation of the Bulk Electric System (BES)."

ReliabilityFirst questions if using the phrase "CIP Exceptional Circumstances" is appropriate here. The definition of 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." ReliabilityFirst believes CIP Exceptional Circumstances criteria are not relative to data transmission.

Likes 0	
Dislikes 0	

Response

George Brown - Acciona Energy North America - 5

Answer	
Document Name	

Comment

1- Generator Operators within the ERCOT footprint who are not also a Qualified Scheduling Entity (QSE) will not be able to comply with the standard as written if their Control Center transmits and receives the data as specified in Requirement R1.

Within the ERCOT footprint the sensitive BES data transmitted between the Control Centers of the Balancing Authority (BA), Transmission Operator (TOP), Reliability Coordinator (RC) and Generator Operator (GOP) is submitted through the QSE (Assume that ERCOT is acting as the RC, BA and/or TOP for particular GOP and that GOP is not also a QSE). The QSE is not a recognized NERC Functional Entity and as such would not be subject to adhering to NERC Reliability Standards. Therefore it would not be possible for a GOP to protect the

sensitive BES data that is transmitted to and from the Control Center of the QSE and ERCOT that ultimately is either being sent or received by the GOP Control Center. NERC CIP-012-1, as written, does not account for this ERCOT nuance. 2 - Pursuant to NERC CIP-012-1, §4 Applicability, this standard is applicable to the Generator Owner. However, the proposed definition of Control Center, exempts the Generator Owner as it only speaks to the Generator Operator's Control Center. NERC CIP-012-1 should not be applicable to the Generator Owner.	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino	
Answer	
Document Name	
Comment	
We seek clarification in the standard verbiage that the intent of this standard applies to inter control center communication. In addition, it would be beneficial to have guidance on key management and inter utility agreements particularly as it pertains to coordination for encryption of data between 3rd parties and compliance impacts on reliability.	
Likes 0	
Dislikes 0	
Response	

Leonard Kula - Independent Electricity System Operator - 2	
Answer	
Document Name	
Comment	

The IESO asserts that the proposed standard does not make clear how entities should work together when addressing security concerns across a communication network link. If both entities work with CIP Standard assumptions on both ends of a communication network, some support for joint handling of issues could be made clear. However, if only one entity is CIP-compliant for a given link, the current standard draft does not make clear the extent of protection expected for the data. The Standard should provide more information on the ownership of obligations for protecting the entire link

It is unclear whether the addition of CIP-012 affects the exemptions of communication networks in any of the applicability sections of other standards (CIP-002 through CIP-011). The IESO requests clarification that CIP-012 fills in some of the gap created the CIP-002 – CIP-011 third party telecommunications exemption (4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.)

It has been ten years since the SANDIA report ("Secure ICCP Considerations and Recommendations"), the only detailed report on this subject which could be considered close having entered mainstream awareness in the industry. Today, as ten years ago, Secure ICCP is not a viable choice for utilities, if only due to limited community experience and vendor support, not to mention the complexities of key management. The transition strategies that SANDIA discusses – Layer 3 protection using IPsec and Layer 2 protection with hardware encryption – remain today's target solutions.

IPsec is a viable alternative. Over MPLS, IPsec could secure GRE tunnels between CE routers. Challenges with this approach include the possibility of having to hire a third party to manage certificates and IPsec links, especially for ISOs that do not manage their own MPLS networks.

The IESO position on security architecture is that business transactions (such as ICCP) should not be tightly coupled with encryption technologies. Solutions should prefer network overlays versus security extensions to a protocol (such as Secure ICCP or DNP3 SA).

The security architecture should prefer least-latent encryption solutions at the Ethernet or IP layers of the network stack. MACsec (802.1AE) models the spirit of an optimal solution within a metro area – could it scale wider?

The IESO's overall position on Secure ICCP is that it represents too much reliability risk. The IESO is concerned about the lack of open standards and protocols available to meet the confidentiality and integrity security objectives of CIP-012. Assuming that a solution involves encryption, the only two open standards and protocols that can meet the CIP-012 security objectives are IPsec and TLS. The potential for vendor leverage in such a small open solution space is large. Vendor-managed MPLS networks, typical among utilities, already entrench high annual telecommunication costs in utility budgets. Security vendors continue to benefit from the expense of establishing layered cyber defenses. Open Source solutions provide a cost and agility refuge from this lopsided value chain without compromising defense layers. The trend toward managed services makes the cost problem worse for utilities, especially in the context of insufficiently evaluated risk. Vendor leverage only grows given the practical consideration that all the communicating parties in a WAN of connected real-time Control Centers would need to adopt a common solution in order to minimize complexity and cost.	
Likes 2	Hydro One Networks, Inc., 1, Farahbakhsh Payam; Hydro One Networks, Inc., 3, Malozewski Paul
Dislikes 0	
Response	
Dermot Smyth - Con Ed - Consolidated Edison Co. of New York - 5, Group Name Con Edison	
Answer	
Document Name	
Comment	
CIP-012-1 should be aligned with TOP-003-3. Data security is already required in TOP-003-3 R5. Only data that is stipulated in the TOP-003-3 R1 data specification for Operational Planning Analysis, Real-time Assessment, and Real-time monitoring should be in scope for CIP-012. The proposed standard does not make clear how entities should work together when addressing security concerns across a communication network link. Some guidance regarding joint handling of communication links would be helpful. Where does the obligation for protecting a link per entity start and end?	
Likes 0	

Dislikes 0	
Response	
Brandon McCormick - Brandon McCormick On Behalf of: Ginny Beigel, City of Vero Beach, 3; Lynne Mila, City of Clewiston, 4; Tom Reedy, Florida Municipal Power Pool, 6; - Brandon McCormick, Group Name FMPA	
Answer	
Document Name	
Comment	
FMPA believes that the proposed standard does not make clear how entities should work together when addressing security concerns across a communication network link. Some support for joint handling of issues should be made clear. FMPA believes that an Implementation Guidance document should be developed and include guidance on possible determination of the security method used being developed at the regional or RC level. This may facilitate a more cost-effective approach. Moreover, the Implementation Guidance could also address the entities evidence needed when they are following what was determined by the Region, RC or ISO.	
Likes 0	
Dislikes 0	
Response	
David Rivera - New York Power Authority - 3	
Answer	
Document Name	
Comment	

The proposed standard does not make clear how entities should work together when addressing security concerns across a communication network link. Some support for joint handling of issues could be made clear. Where does the obligation for protecting a link per entity start and end?

Note: These comments are equivalent to those submitted by the NPCC/TFIST group, except for changes in the Yes/No answers.

Likes 0	
Dislikes 0	
Response	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	
Document Name	
Comment	

1. The NSRF questions the use of “Real-time monitoring” as an applicable object within R1. “Real-time” is defined as “present time as opposed to future time”. Which our industry understands and without the word “monitoring” being defined, may lead to misinterpretation by responsible entities and CEAs, alike. The word “monitoring” may mean ALL monitoring of an entity’s entire SCADA system. It should be the “monitoring” of BES data, only, that is required for Operational Planning Analysis and Real-time Assessments.

2. The Applicability section states, “For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly”. This proposed Standard does not specify any specific entities and we recommend that this is removed.

3. The NSRF has concerns with the proposed definition of Control Center. The largest issue is the last paragraph concerning a Generating Operator. The use of the word “capability” is ambiguous and will confuse Registered Entities and CEAs, a like. The SDT should consider the approved Applicability within PER-005-2 part 4.1.5.1, which reads:

Dispatch personnel at a centrally located dispatch center who receive direction from the Generator Operator's Reliability Coordinator, Balancing Authority, Transmission Operator, or Transmission Owner, and may develop specific dispatch instructions for plant operators under their control. This personnel does not include plant operators located at a generator plant site or personnel at a centrally located dispatch center who relay dispatch instructions without making any modifications.

This aligns with current and understood wording of PER-005-2.

4. Are the noted "Real-time reliability related- tasks" within the proposed definition, the same "Real-time Reliability-related task prescribed in PER-005-2? If so, please state this in your consideration of comments document and within your guidance document.

5. The NSRF believes that data associated with Operational Planning Analyses (OPA), Real-time monitoring (RTm), and Real-time Assessments (RTA) are predicated on other Standards and protection of data is required but all three areas (OPA, RTm, and RTA) are not subject equally to the Applicable Entities noted in CIP-012-1. Per IRO-010-2, R1, the RC is to document its specifications necessary for OPA, RTm, and RTA. Per TOP-003-3, R1 the TOP is to document its specifications necessary for OPA, RTm, and RTA. Per TOP-003-3, R2, the BA is to document its specifications necessary for analysis functions and RTm, only. The SDT, in the Technical Rationale and Justification document, acknowledges TOP-003 and IRO-010 "provides consistent scoping of identified data" [R1 section: Alignment with IRO and TOP Standards"]. The SDT should quantify that the data to be protected is the data associated with the Applicable entities with IRO-010-2 and TOP-003-3. With doing this, the SDT will articulate what the entity is to perform what analysis and what "data" is to be protected, based on already approved NERC Reliability Standards. By clearly identifying (and linking) the data to be protected from the data specifications developed under Standards TOP-003 and IRO-010, there is no room for interpretation of what "data" is to be protected.

Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	

Comment
Although the FERC order specifies data between Control Centers, Texas RE notes that there is OPA, RTA, Real-time monitoring data that is not between control centers. For example, Distribution Providers provide BES sensitive data but would not be subject the standard. Also there are numerous GOPs that do not have a control center per the definition that provide BES sensitive data which also would not subject to CIP-012-1. Texas RE is concerned this creates a reliability gap since these scenarios would not be covered under the proposed draft of CIP-012-1. Although Texas RE does not oppose a CIP Exceptional Circumstances exception from the implementation requirements set forth in CIP-012-1 R2, Texas RE requests that the SDT provide a rationale for why such an exception is appropriate. In particular, it is unclear why certain CIP exception conditions, such as an imminent hardware failure, should necessarily trigger a relaxation of physical security protections for communications links transmitted sensitive data in all circumstances.

Likes 0	
Dislikes 0	

Response

Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	
Document Name	

Comment
See APPA Comments.

Likes 0	
Dislikes 0	

Response

Chris Scanlon - Exelon - 1	
Answer	
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Marty Hostler - Northern California Power Agency - 5	
Answer	
Document Name	
Comment	
Refer to APPA, TAPs, and Utility Services comments.	
Likes 0	
Dislikes 0	
Response	
Dennis Sismaet - Northern California Power Agency - 6	
Answer	
Document Name	

Comment	
Refer to APPA, TAPs, and Utility Services comments.	
Likes 0	
Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 3	
Answer	
Document Name	
Comment	
AZPS reiterates its comments provided in response to Requirement R1 regarding clear delineation of responsibilities between receiving and transmitting entities. Because the potential impacts of a receiving entity not appropriately implementing the technology needed for decryption or use of protected data sent by a transmitting entity lie outside of the proposed Requirement R1 in real-time data and assessment obligations, placement of the obligations for Requirement R1 on the transmitting is appropriate and reduces the potential for double jeopardy and/or "waterfall" non-compliance events. Hence, AZPS suggests that it is appropriate to place the obligation for Requirement R1 on the transmitting entity. Finally, AZPS reiterates the NERC ORD as a reference guide and resource regarding the scope of this standard and sensitive data generally. The NERC ORD Agreement has long maintained an accepted, well-established definition for sensitive reliability data. That definition does not include data utilized in the Operational Planning Horizon and, for the reasons discussed above, AZPS asserts that the inclusion of Operational Planning Analysis in Requirement R1 extends the scope of BES sensitive data without attendant benefit to reliability. AZPS recommends the deletion of Operational Planning Analysis from Requirement R1 to allow the Requirement to remain consistent with well-established, well understood precedent as set forth in the NERC ORD Agreement.	
Likes 0	

Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	
Document Name	
Comment	
Clarification needed – Does 'data used for Operational Planning Analysis, Real-time Assessments, and Real-time monitoring ' include Generator Unit Commitment Data and/or transmission and generator outages which are posted publicly?	
Likes 0	
Dislikes 0	
Response	
Aaron Austin - AEP - 3	
Answer	
Document Name	CIP-012-1 – Cyber Security -Communication Networks Diagram.doc
Comment	
AEP suggests these should be added to the diagram as clearly in scope.	
Likes 0	
Dislikes 0	
Response	

Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	
Document Name	
Comment	
NRECA appreciates the continuing efforts of the SDT.	
Likes 0	
Dislikes 0	
Response	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	
Document Name	
Comment	
The proposed standard does not make clear how entities should work together when addressing security concerns across a communication network link. Some support for joint handling of issues could be made clear. Where does the obligation for protecting a link per entity start and end?	
Likes 0	
Dislikes 0	
Response	
Lona Calderon - Salt River Project - 1,3,5,6 - WECC	

Answer	
Document Name	
Comment	

One challenge associated with CIP-012-1 is industry-wide coordination would be necessary to successfully implement encryption.

In addition to adding latency, encryption adds burden for ongoing maintenance and management for an encryption program. SRP agrees with LPPC that guidance is needed on key management and inter utility agreements pertaining to coordination for encryption of data and impacts on real-time operation of the Bulk Electric System.

Likes 0	
Dislikes 0	
Response	
Thomas Breene - WEC Energy Group, Inc. - 3	
Answer	
Document Name	
Comment	

1. We question the use of “Real-time monitoring” as an applicable object within R1. “Real-time” is defined as “present time as opposed to future time”. Which our industry understands and without the word “monitoring” being defined, may lead to misinterpretation by responsible entities and CEAs, alike. The word “monitoring” may mean ALL monitoring of an entity’s entire SCADA system. It should be the “monitoring” of BES data, only, that is required for Operational Planning Analysis and Real-time Assessments.

2. The Applicability section states, “For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly”. This proposed Standard does not specify any specific entities and recommend that this be removed.

3. We have concerns with the proposed definition of Control Center. The largest issue is the last paragraph concerning a Generating Operator. The use of the word "capability" is ambiguous and will confuse Registered Entities and CEAs, a like. The SDT should consider the approved Applicability within PER-005-2 part 4.1.5.1, which reads:

Dispatch personnel at a centrally located dispatch center who receive direction from the Generator Operator's Reliability Coordinator, Balancing Authority, Transmission Operator, or Transmission Owner, and may develop specific dispatch instructions for plant operators under their control. These personnel do not include plant operators located at a generator plant site or personnel at a centrally located dispatch center who relay dispatch instructions without making any modifications.

This aligns with current and understood wording of PER-005-2.

4. Are the noted "Real-time reliability related- tasks" within the proposed definition, the same "Real-time Reliability-related task prescribed in PER-005-2? If so, please state this in your consideration of comments document and within your guidance document.

5. We believe that data associated with Operational Planning Analyses (OPA), Real-time monitoring (RTm), and Real-time Assessments (RTA) are predicated on other Standards and protection of data is required but all three areas (OPA, RTm, and RTA) are not subject equally to the Applicable Entities noted in CIP-012-1. Per IRO-010-2, R1, the RC is to document its specifications necessary for OPA, RTm, and RTA. Per TOP-003-3, R1 the TOP is to document its specifications necessary for OPA, RTm, and RTA. Per TOP-003-3, R2, the BA is to document its specifications necessary for analysis functions and RTm, only. The SDT, in the Technical Rationale and Justification document acknowledges TOP-003 and IRO-010 "provides consistent scoping of identified data" [R1 section: Alignment with IRO and TOP Standards"]. The SDT should quantify that the data to be protected is the data associated with the Applicable entities with IRO-010-2 and TOP-003-3. With doing this, the SDT will articulate what the entity is to preform what analysis and what "data" is to be protected, based on already approved NERC Reliability Standards. By clearly identifying (and linking) the data to be protected from the data specifications developed under Standards TOP-003 and IRO-010, there is no room for interpretation of what "data" is to be protected.

Likes 0	
Dislikes 0	
Response	
Russell Noble - Cowlitz County PUD - 3	

Answer	
Document Name	
Comment	
Although Cowlitz PUD agrees with the intent of the proposed standard, we are concerned the protective measures developed by entities could have unintended consequences. In particular, there is concern encryption could unacceptably slow data transmission.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Con-Edison and Dominion	
Answer	
Document Name	
Comment	
· The proposed standard does not make clear how entities should work together when addressing security concerns across a communication network link. Some support for joint handling of issues could be made clear. Where does the obligation for protecting a link per entity start and end?	
Likes 0	
Dislikes 0	
Response	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	

Document Name	
Comment	

ERCOT ISO signs on to the ITC SWG comments:

The ITC SWG asserts that the proposed standard does not make clear how entities should work together when addressing security concerns across a communication network link. If both entities work with CIP Standard assumptions on both ends of a communication network, some support for joint handling of issues could be made clear. However, if only one entity is CIP-compliant for a given link, the current standard draft does not make clear the extent of protection expected for the data. The Standard should provide more information on the ownership of obligations for protecting the entire link.

It is unclear whether the addition of CIP-012 affects the exemptions of communication networks in any of the applicability sections of other standards (CIP-002 through CIP-011). The SWG requests clarification that CIP-012 fills in some of the gap created the CIP-002 – CIP-011 third party telecommunications exemption (4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.)

It has been ten years since the SANDIA report ("Secure ICCP Considerations and Recommendations"), the only detailed report on this subject which could be considered close having entered mainstream awareness in the industry. Today, as ten years ago, Secure ICCP is not a viable choice for utilities, if only due to limited community experience and vendor support, not to mention the complexities of key management. The transition strategies that SANDIA discusses – Layer 3 protection using IPsec and Layer 2 protection with hardware encryption – remain today's target solutions.

WECC, and specifically the WECC DEMSWG (Data Exchange and EMS Working Group) has been working with Pacific Northwest National Laboratory (PNNL) for some time on a new evaluation of Secure ICCP. PNNL recently completed their work and presented the results to DEMSWG in 2016. The PNNL study functionally succeeded but with enough limitations that PNNL was prompted to conclude that it would be difficult to make a business case for implementing Secure ICCP when other solutions are available.

IPsec is a viable alternative. Over MPLS, IPsec could secure GRE tunnels between CE routers. Challenges with this approach include the possibility of having to hire a third party to manage certificates and IPsec links, especially for ISOs that do not manage their own MPLS networks.

The ITC SWG position on security architecture is that business transactions (such as ICCP) should not be tightly coupled with encryption technologies. Solutions should prefer network overlays versus security extensions to a protocol (such as Secure ICCP or DNP3 SA). The security architecture should prefer least-latent encryption solutions at the Ethernet or IP layers of the network stack. MACsec (802.1AE) models the spirit of an optimal solution within a metro area – could it scale wider? The ITC SWG's overall position on Secure ICCP is that it represents too much reliability risk. The ITC SWG is concerned about the lack of open standards and protocols available to meet the confidentiality and integrity security objectives of CIP-012. Assuming that a solution involves encryption, the only two open standards and protocols that can meet the CIP-012 security objectives are IPsec and TLS. The potential for vendor leverage in such a small open solution space is large. Vendor-managed MPLS networks, typical among utilities, already entrench high annual telecommunication costs in utility budgets. Security vendors continue to benefit from the expense of establishing layered cyber defenses. Open Source solutions provide a cost and agility refuge from this lopsided value chain without compromising defense layers. The trend toward managed services makes the cost problem worse for utilities, especially in the context of insufficiently evaluated risk. Vendor leverage only grows given the practical consideration that all the communicating parties in a WAN of connected real-time Control Centers would need to adopt a common solution in order to minimize complexity and cost.	
Likes 0	
Dislikes 0	
Response	
Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 3	
Answer	
Document Name	
Comment	
Tacoma Power supports the comments of APPA	
Likes 0	
Dislikes 0	

Response	
Theresa Rakowsky - Puget Sound Energy, Inc. - 1	
Answer	
Document Name	
Comment	
n/a	
Likes 0	
Dislikes 0	
Response	
Jack Cashin - American Public Power Association - 4	
Answer	
Document Name	
Comment	
APPA believes that the proposed standard does not make clear how entities should work together when addressing security concerns across a communication network link. Some support for joint handling of issues should be made clear. Public power believes that an Implementation Guidance document should be developed and include guidance on possible determination of the security method used being developed at the regional or RC level. This may facilitate a more cost-effective approach. Moreover, the Implementation Guidance could also address the entities evidence needed when they are following what was determined by the Region, RC or ISO.	
Likes 0	

Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	
Document Name	
Comment	
The STD should consider changing the title of the CIP-012-1 requirement to "CIP-012-1-Cyber Security – Control Center Communication **Links**" to align with the language in FERC Order No. 822 and the language in Requirement R1. The current use of the term "Networks" may be misleading because it implies a broader scope of communication. Additionally, the violation severity levels (VSL) for this requirement is limited to "Severe". CenterPoint Energy recommends that Requirement R1 VSL be "Moderate" to "High" due to the fact that Requirement R1 is a documentation requirement.	
Likes 0	
Dislikes 0	
Response	
David Greene - SERC Reliability Corporation - 10, Group Name SERC CIPC	
Answer	
Document Name	
Comment	
NA	
Likes 0	

Dislikes 0	
Response	
Warren Cross - ACES Power Marketing - 1,3,4,5 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standards Collaborators	
Answer	
Document Name	
Comment	
We thank you for this opportunity to provide these comments.	
Likes 0	
Dislikes 0	
Response	
Sheranee Nedd - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	
Document Name	
Comment	
PSEG supports the NPCC comments.	
Likes 1	PSEG - PSEG Fossil LLC, 5, Kucey Tim
Dislikes 0	
Response	

Michael Puscas - ISO New England, Inc. - 2	
Answer	
Document Name	
Comment	

Comments:

- The proposed standard does not make clear how entities should work together when addressing security concerns across a communication network link. If both entities work with CIP Standard assumptions on both ends of a communication network, some support for joint handling of issues could be made clear. However, if only one entity is CIP-compliant for a given link, the current standard draft does not make clear the extent of protection expected for the data. Where does the obligation for protecting a link per entity start and end?
- Does the addition of CIP-012 affect the exemptions of communication networks in any of the applicability sections of other standards (CIP-002 through CIP-011)?
- While the CIP standards should emphasize outcomes and allow entities to achieve specific security objectives in many ways, protections applied to communications should be evaluated with due consideration of the context in which people, processes and technology are applied to establish a given security protection. Demonstration of risk mitigation should include assessment of not just technology and process to provide protection, but also the diversity and severity of threats present in a given context (e.g. the difference between dedicated communication links as opposed to broadly shared communications infrastructure). Particular technology and process applied in a context with fewer or lower likelihood threats should be preferred over the same technology and process in a context with more or greater likelihood threats (i.e. greater overall risk). Simply specifying that some (how much?) risk mitigation should be applied by means that include physical, logical and possibly other means leads to insufficient conditions for establishing compliance both for the responsible entity and anyone reviewing compliance for that entity. Entities should consider not only that risk mitigation should take place, but also the thresholds for residual risk that should be considered acceptable for such communication.
- It should be noted that in a recent report from the National Infrastructure Advisory Council (NIAC) to the DHS and President of the United States, the NIAC recommended that separate communication networks be used for critical communications (reference

https://www.dhs.gov/publication/niac-securing-cyber-assets-addressing-urgent-cyber-threats-critical-infrastructure-final, report page 3, first recommendation).	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	
Document Name	
Comment	
BPA suggests adding the verbiage “where technically feasible” to the requirements, in order to implement controls where appropriate, based on the technology (as discussed in Q1) and risk.	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	
Document Name	
Comment	

Utility Services believes that the proposed standard does not make clear how entities should work together when addressing security concerns across a communication network link. Some support for joint handling of issues should be made clear. Utility Services believes that an Implementation Guidance document should be developed and include guidance on possible determination of the security method used being developed at the regional or RC level. This may facilitate a more cost-effective approach. Moreover, the Implementation Guidance could also address the entities evidence needed when they are following what was determined by the Region, RC or ISO.

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	
Comment	
If the SDT retains a data-centric approach, we believe the time element is very important and is correctly captured in the requirement with the phrase “while being transmitted between Control Centers.” We encourage the SDT to retain this language. We note the RSAW drops the time element and just says “transmitted between”. The time element is very important, as data transmitted between Control Centers a year ago is not the focus of this standard. This will, ideally, be reflected in the Standard itself, as well as the Technical Rationale and the RSAW, for clarity.	
Likes 0	
Dislikes 0	
Response	

David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	
Document Name	
Comment	
OPG understands the focus is on protection of data communication between control centers but would like to clarify that it is not being required to verify integrity of data from it's origination points to the point where it's first aggregated at a control center, as this would be a substantially more difficult and costly requirement to achieve.	
Likes 0	
Dislikes 0	
Response	

Ronald Donahey - TECO - Tampa Electric Co. - 3	
Answer	
Document Name	
Comment	
Tampa Electric appreciates the efforts of the Standards Drafting Team in developing protections for Communication Networks. We have concerns that the scope of the standard regarding data protection (based on IRO-010 and TOP-003) extends the requirement to data/information that is not currently required to be protected at the level of a High Impact BES Cyber System. This approach does not match the intent and protections of all other NERC CIP standards.	
Likes 0	
Dislikes 0	
Response	

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	
Document Name	
Comment	
The SPP Standards Review Group recommends the drafting team verifies and confirms that the NERC defined terms 'Operational Planning Analyses', 'Real-time Assessments', and 'Real-time' (mentioned in the Rationale Section in reference to Requirement R1) are defined and properly aligned with the Rules of Procedure (RoP) documentation. We have a concern that if the terms aren't properly defined and aligned in both documents that this could lead to potential interpretation issues for future projects. During the verification process, should the drafting team discover that there is supporting evidence to SPP's concerns, we would recommend the drafting team developing a Standard Authorization Request (SAR) to help ensures that both documents have consistency in the definition of the terms mentioned. The SPP Standard Review Group would ask the drafting team to provide clarity on why the RoP is not mentioned in the Implementation Plan like the NERC Glossary of Terms. From our perspective, the RoP and the definitions, it contains have the same significance that the Glossary of Terms have in reference to the industry defined terms.	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 5	
Answer	
Document Name	
Comment	

Reclamation recommends the SDT define the term “Real-time monitoring” in the NERC Glossary of Terms. The Applicability section states, “For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.” No Requirements in this proposed Standard explicitly specify a functional entity or entities; therefore, Reclamation also recommends that this sentence be removed.	
Likes 0	
Dislikes 0	
Response	
Scott Berry - Scott Berry On Behalf of: Jack Alvey, Indiana Municipal Power Agency, 1, 4; - Scott Berry	
Answer	
Document Name	2016-02_Unofficial_Comment_Form_Control_Center_Definition_08142017.docx
Comment	
IMPA is attaching its comments for Control Center. The feedback/survey sheet is not linked to this vote. Our Control Center survey response is attached.	
Likes 0	
Dislikes 0	
Response	
Lauren Price - American Transmission Company, LLC - 1	
Answer	
Document Name	
Comment	

Not Applicable	
Likes 0	
Dislikes 0	
Response	
Laura McLeod - NB Power Corporation - 5	
Answer	
Document Name	
Comment	
No additional comments.	
Likes 0	
Dislikes 0	
Response	
Haley Sousa - Public Utility District No. 1 of Chelan County - 5	
Answer	
Document Name	
Comment	
Implementing industry-wide secure communication is a significant coordination challenge for entities and their associated vendors. The increase in security also brings increased complexity, maintenance, and failure potential that may negatively impact the reliable	

operation of the BES. As a result, coordination for encryption key management will become an essential activity and CHPD would, similar to other entity comments, appreciate guidance for these activities.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb On Behalf of: Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 3, 5, 1, 6; James McBee, Great Plains Energy - Kansas City Power and Light Co., 3, 5, 1, 6; Jessica Tucker, Great Plains Energy - Kansas City Power and Light Co., 3, 5, 1, 6; Jim Flucke, Great Plains Energy - Kansas City Power and Light Co., 3, 5, 1, 6; - Douglas Webb	
Answer	
Document Name	
Comment	
None.	
Likes 0	
Dislikes 0	
Response	
Janis Weddle - Public Utility District No. 1 of Chelan County - 6	
Answer	
Document Name	
Comment	

Implementing industry-wide secure communication is a significant coordination challenge for entities and their associated vendors. The increase in security also brings increased complexity, maintenance, and failure potential that may negatively impact the reliable operation of the BES. As a result, coordination for encryption key management will become an essential activity and CHPD would, similar to other entity comments, appreciate guidance for these activities.

Likes 0	
Dislikes 0	
Response	

Comments from David Greene, SERC

Questions

1. Requirement R1: The SDT drafted CIP-012-1 Requirement R1 to meet the mandatory requirement for the Responsible Entity to develop one or more documented plan(s) to mitigate the risk of the unauthorized disclosure or modification of data used for Operational Planning Analysis, Real-time Assessment, and Real-time monitoring data while being transmitted between Control Centers. Do you agree with this revision? If not, please provide the basis for your disagreement and an alternate proposal.

   ☐ Yes
   ☒ No
   Comments:

   - **Revise R1.** First paragraph, remove "Operational Planning Analysis"

   Rationale: Operational Planning Analysis data does not impact the BES within 15 minutes. The systems handling Operational Planning Analysis data are typically separate from the systems performing real-time BES analysis/control.

The data involved with Operational Planning is “theoretical”, e.g., requests to take a line out of service or de-rate a generation unit. If an event occurs in real-time to trip a line or de-rate a unit, information is immediately conveyed via a mechanism other than Operational Planning data.

Because the Operational Planning data is requesting permission to do something, the request will be validated by other measures – e.g., permission to take the line out of service/de-rate the unit, followed (later) by switching orders to take the line out of service or revised bid into the generation market indicating the unit will only provide the de-rated output.

Thus, because it does not directly impact the reliable operation of the BES and cross-checks are already built into the data process, stringent controls for data transfer is not required.

2. Requirement R1: The SDT seeks comment on the need to scope sensitive BES data as it applies to Operational Planning Analysis, Real-time Assessment, and Real-time monitoring. Do you agree with scoping CIP-012-1 Requirement R1 in this manner? Please provide comment in support of your response.

☐ Yes
☒ No
Comments:

- **Revise R1.** First paragraph, remove “Operational Planning Analysis”

Rationale: Operational Planning Analysis data does not impact the BES within 15 minutes. The systems handling Operational Planning Analysis data are typically separate from the systems performing real-time BES analysis/control.

The data involved with Operational Planning is “theoretical”, e.g., requests to take a line out of service or de-rate a generation unit. If an event occurs in real-time to trip a line or de-rate a unit, information is immediately conveyed via a mechanism other than Operational Planning data.

Because the Operational Planning data is requesting permission to do something, the request will be validated by other measures – e.g., permission to take the line out of service/de-rate the unit, followed (later) by switching orders to take the line out of service or revised bid into the generation market indicating the unit will only provide the de-rated output.

Thus, because it does not directly impact the reliable operation of the BES and cross-checks are already built into the data process, stringent controls for data transfer is not required.

3. Implementation Plan: The SDT revised the Implementation Plan such that the standard and NERC Glossary terms are effective the first day of the first calendar quarter that is twelve (12) calendar months after the effective date of the applicable governmental authority's order approving the standard, or as otherwise provided for by the applicable governmental authority. Do you agree with this proposal? If you agree with the proposed implementation time period, please note the actions you will take that require this amount of time to complete. If you think an alternate implementation time period is needed – shorter or longer - please propose an alternate implementation plan and provide a detailed explanation of actions and time needed to meet the implementation deadline.

   ☐ Yes
   ☒ No
   Comments:

   - **Alternate Implementation Period**: 2 Year Implementation Plan Period

   Rationale: There are a number of factors to consider, and all affect the time required to implement, to include the following:
   - Complexity of the technology solutions to be implemented,
   - Number of interconnecting lines to secure,
   - Troubleshooting/testing at each connection point, and
   - Coordination requirements with external stakeholders

4. The SDT believes proposed CIP-012-1 provides entities with flexibility to meet the reliability objectives in a cost effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost effective approaches, please provide your recommendation and, if appropriate, technical justification.

   ☒ Yes
   ☐ No
   Comments:

5. If you have additional comments on the proposed CIP-012-1 – Cyber Security -- Communication Networks drafted in response to the FERC directive that you have **not** provided in response to the questions above, please provide them here.

   Comments: NA

Comments from Vivian Vo, APS

Questions

1. Requirement R1: The SDT drafted CIP-012-1 Requirement R1 to meet the mandatory requirement for the Responsible Entity to develop one or more documented plan(s) to mitigate the risk of the unauthorized disclosure or modification of data used for Operational Planning Analysis, Real-time Assessment, and Real-time monitoring data while being transmitted between Control Centers. Do you agree with this revision? If not, please provide the basis for your disagreement and an alternate proposal.

   ☒ Yes
   ☐ No
   Comments:

   AZPS respectfully submits that, as written, the allocation of responsibilities between transmitting and receiving entities is unclear. Delineation of these responsibilities is essential because a receiving entity has no control over the behavior, implementation, and/or lack of implementation of third-party entities and cannot prevent third-party entities from transmitting unprotected data. As written, Requirement R1 could be construed as holding both the transmitting and receiving entity responsible where the transmitting entity fails to implement its plan. The receiving entity would only be aware/in receipt of the protected or unprotected data once it is transmitted by the transmitting entity. At which point, the potential for non-compliance has already occurred. Accordingly, because the data emanates from the transmitting entity, the data protection obligation should emanate from the transmitting entity.

   For this reason, Requirement R1 should not hold receiving entities responsible for receiving data from another entity that failed to implement its plan. Responsibility for CIP-012-1 R1 should be placed clearly upon the transmitting entity and AZPS requests that the

SDT modify Requirement R1 to ensure that there is a clear allocation of responsibilities between the transmitting and receiving entities. AZPS submits for consideration by the SDT a revised Requirement R1 below with language clarifying the allocation of responsibilities

R1. The Responsible Entity shall develop one or more documented plan(s) to mitigate the risk of the unauthorized disclosure or modification of data used for Operational Planning Analysis, Real-time Assessments, and Real-time monitoring ~~while being transmitted~~ when transmitting data from one Control Center to another Control Center ~~between Control Centers~~. This excludes oral communications. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

The above proposed revisions clarify allocation of responsibilities without compromising on the level of required protection and while maintaining recognition that meaningful, logically protected communication that can be decrypted for use by the receiving entity requires bilateral agreement between the transmitting entity and receiving entity.

Comments from Scott Berry, Indiana Municipal Power Agency

Proposed Definition of "Control Center"

Revised Definition:
One or more facilities, including their associated data centers, that monitor and control the Bulk Electric System (BES) and host operating personnel who perform Real-time reliability-related tasks of: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for Transmission Facilities at two or more locations, or 4) a Generator Operator for generation Facilities at two or more locations.

For Reliability Coordinators, Balancing Authorities, and Transmission Operators, the operating personnel above are System Operators.

For Transmission Owners performing the Real-time reliability-related tasks of a Transmission Operator, the operating personnel above consist of personnel, excluding field switching personnel, who can act independently to operate or direct the operation of the Transmission Owner's Bulk Electric System Transmission Facilities in Real-time.

For Generator Operators, the operating personnel above consist of dispatch personnel at a centrally located dispatch center who receive direction from the Generator Operator's Reliability Coordinator, Balancing Authority, Transmission Operator, or Transmission Owner, and have the capability to develop specific dispatch instructions for plant operators under their control. These personnel do not include plant operators located at a generator plant site or personnel at a centrally located dispatch center who relay dispatch instructions without making any modifications.

Redline Definition:

One or more facilities, including their associated data centers, that monitor and control the Bulk Electric System (BES) and host ~~hosting~~ operating personnel ~~that monitor and control the Bulk Electric System (BES) in real-time to~~ who perform ~~the~~ Real-time reliability-related tasks~~, including their associated data centers,~~ of: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for Transmission Facilities at two or more locations, or 4) a Generator Operator for generation Facilities at two or more locations.

For Reliability Coordinators, Balancing Authorities, and Transmission Operators, the operating personnel above are System Operators.

For Transmission Owners performing the Real-time reliability-related tasks of a Transmission Operator, the operating personnel above consist of personnel, excluding field switching personnel, who can act independently to operate or direct the operation of the Transmission Owner's Bulk Electric System Transmission Facilities in Real-time.

For Generator Operators, the operating personnel above consist of dispatch personnel at a centrally located dispatch center who receive direction from the Generator Operator's Reliability Coordinator, Balancing Authority, Transmission Operator, or Transmission Owner, and have the capability to develop specific dispatch instructions for plant operators under their control. These personnel do not include plant operators located at a generator plant site or personnel at a centrally located dispatch center who relay dispatch instructions without making any modifications.

Currently Approved Definition:

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, of: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for transmission Facilities at two or more locations, or 4) a Generator Operator for generation Facilities at two or more locations.

End of Report

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2016-01 Modifications to CIP Standards
CIP-012-1

Draft Reliability Standard Audit Worksheet (RSAW) Posted for Industry Comment through September 11, 2017

Now Available

The draft RSAW for **CIP-012-1 – Cyber Security – Control Center Communication Networks** is posted on the project page for industry comment through **8 p.m. Eastern, Monday, September 11, 2017.** Submit feedback regarding the draft RSAW to RSAWfeedback@nerc.net.

For more information or assistance, contact Standards Developers, Katherine Street at (404) 446-9702 or Mat Bunch at (404) 446-9785.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Proposed Definition of: "Control Center"

Term: "Control Center"

Revised Definition:

One or more facilities, including their associated data centers, that monitor and control the Bulk Electric System (BES) and host operating personnel who perform Real-time reliability-related tasks of: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for Transmission Facilities at two or more locations, or 4) a Generator Operator for generation Facilities at two or more locations.

For Reliability Coordinators, Balancing Authorities, and Transmission Operators, the operating personnel above are System Operators.

For Transmission Owners performing the Real-time reliability-related tasks of a Transmission Operator, the operating personnel above consist of personnel, excluding field switching personnel, who can act independently to operate or direct the operation of the Transmission Owner's Bulk Electric System Transmission Facilities in Real-time.

For Generator Operators, the operating personnel above consist of dispatch personnel at a centrally located dispatch center who receive direction from the Generator Operator's Reliability Coordinator, Balancing Authority, Transmission Operator, or Transmission Owner, and have the capability to develop specific dispatch instructions for plant operators under their control. These personnel do not include plant operators located at a generator plant site or personnel at a centrally located dispatch center who relay dispatch instructions without making any modifications.

Redline Definition:

One or more facilities, including their associated data centers, that monitor and control the Bulk Electric System (BES) and host~~hosting~~ operating personnel ~~that monitor and control the Bulk Electric System (BES) in real-time to~~ who perform ~~the~~ Real-time reliability related--tasks~~, including their associated data centers,~~ of: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for ~~transmission~~Transmission Facilities at two or more locations, or 4) a Generator Operator for generation Facilities at two or more locations.

For Reliability Coordinators, Balancing Authorities, and Transmission Operators, the operating personnel above are System Operators.

For Transmission Owners performing the Real-time reliability--related tasks of a Transmission Operator, the operating personnel above consist of personnel, excluding field switching personnel, who can act independently to operate or direct the operation of the Transmission Owner's Bulk Electric System ~~transmission~~Transmission Facilities in Real-time.

For Generator Operators, the operating personnel above consist of dispatch personnel at a centrally located dispatch center who receive direction from the Generator Operator's Reliability Coordinator, Balancing Authority, Transmission Operator, or Transmission Owner, and have the capability to develop specific dispatch instructions for plant operators under their control. These personnel do not include plant operators located at a generator plant site or personnel at a centrally located dispatch center who relay dispatch instructions without making any modifications.

Currently Approved Definition:

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, of: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for transmission Facilities at two or more locations, or 4) a Generator Operator for generation Facilities at two or more locations.

DRAFT

Cyber Security Control Center Communication Plans

Technical Rationale and Justification for Reliability Standard CIP-012-1

August 11, 2017

Table of Contents

Introduction

On January 21, 2016, the Federal Energy Regulatory Commission (FERC or Commission) issued Order No. 822, approving seven Critical Infrastructure Protection (CIP) Reliability Standards and new or modified terms in the Glossary of Terms Used in NERC Reliability Standards, and directing modifications to the CIP Reliability Standards. Among others, the Commission directed the North American Electric Reliability Corporation (NERC) to "develop modifications to the CIP Reliability Standards to require Responsible Entities[1] to implement controls to protect, at a minimum, communication links and sensitive bulk electric system data communicated between bulk electric system Control Centers in a manner that is appropriately tailored to address the risks posed to the bulk electric system by the assets being protected (i.e., high, medium, or low impact)." (Order 822, Paragraph 53)

In response to the directive in Order No. 822, the Project 2016-02 standard drafting team (SDT) drafted Reliability Standard CIP-012-1 to require Responsible Entities to implement controls to protect sensitive Bulk Electric System (BES) data and communications links between BES Control Centers. Due to the sensitivity of the data being communicated between Control Centers, as defined in the Glossary of Terms Used in NERC Reliability Standards, the standard applies to all impact levels (i.e., high, medium, or low impact).

The SDT drafted requirements to provide Responsible Entities the latitude to protect the communication links, the data, or both, to satisfy the security objective consistent with the capabilities of the Responsible Entity's operational environment. Requirement R1 requires Responsible Entities to document one or more plans that protect Operational Planning Analysis, Real-time Assessment, and Real-time monitoring data while being transmitted between Control Centers. The plan(s) must address how the Responsible Entity will mitigate the risk of unauthorized disclosure or modification of the applicable data. Requirement R2 covers implementation of the plan developed according to Requirement R1.

This technical rationale and justification document explains the technical rationale for the proposed Reliability Standard to provide stakeholders and the ERO Enterprise an understanding of the technology and technical requirements in the Reliability Standard. It also contains information on the SDT's intent in crafting the requirements.

[1] As used in the CIP Standards, a Responsible Entity refers to the registered entities subject to the CIP Standards.

Requirement R1

R1. *The Responsible Entity shall develop one or more documented plan(s) to mitigate the risk of the unauthorized disclosure or modification of data used for Operational Planning Analysis, Real-time Assessments, and Real-time monitoring while being transmitted between Control Centers. This excludes oral communications. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1 *Risk mitigation shall be accomplished by one or more of the following actions:*

- *Physically protecting the communication links transmitting the data;*
- *Logically protecting the data during transmission; or*
- *Using an equally effective method to mitigate the risk of unauthorized disclosure or modification of the data.*

Note: If the Responsible Entity does not have a Control Center or it does not transmit the type of data specified in Requirement R1 of CIP-012-1 between two Control Centers, the requirements in CIP-012-1 would not apply to that entity.

General Considerations for Requirement R1

The focus of Requirement R1 is on developing a plan to protect information that is critical to the real-time operations of the Bulk Electric System while in transit between applicable Control Centers.

Overview of confidentiality and integrity

The SDT drafted CIP-012-1 to address confidentiality and integrity of data used for Operational Planning Analysis, Real-time Assessment, and Real-time monitoring. This is accomplished by drafting the requirement to mitigate the risk from unauthorized disclosure (confidentiality) or modification (integrity). For this Standard, the SDT relied on the definitions of confidentiality and integrity as defined by National Institute of Standards and Technology (NIST).

- Confidentiality is defined as, "Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information."[2]
- Integrity is defined as, "Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity."[3]

The SDT asserts that the availability of this data is already required by the performance obligation of the Operating and Planning Reliability Standards. The SDT drafted CIP-012 to address the data while being transmitted. The SDT maintains that this data resides within BES Cyber Systems, and while at rest is protected by CIP-003 through CIP-011.

Alignment with IRO and TOP standards

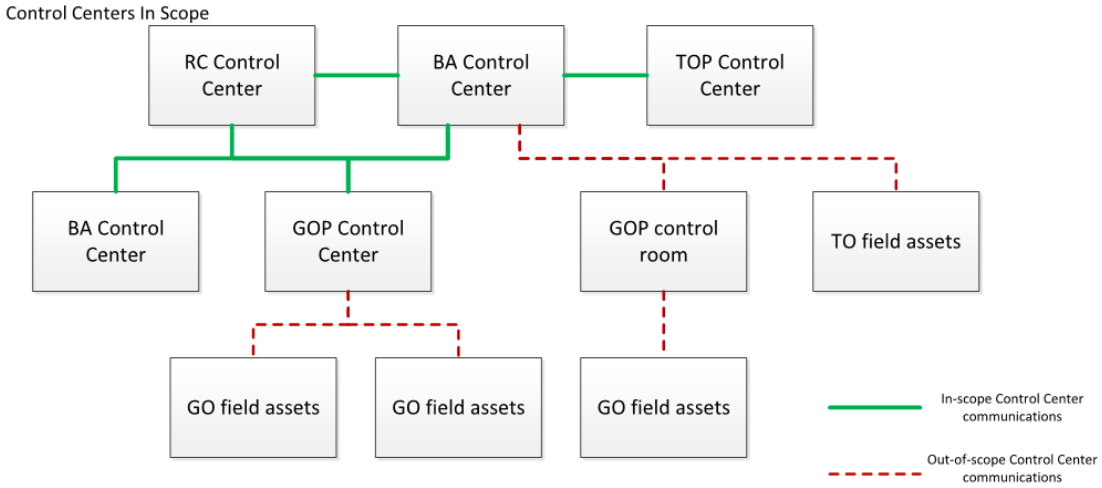
The SDT noted the FERC reference to additional Reliability Standards and the responsibilities to protect the data in accordance with those standards (TOP-003 and IRO-010). The SDT used these references to drive the identification of sensitive BES data and chose to base the CIP-012 requirements on the data specifications in these standards. This approach provides consistent scoping of identified data, and does not require each entity to devise its own list or inventory of this data. Many entities are required to provide this data under agreements executed with their RC, BA or TOP, often without benefit of knowing how those entities use that data.

[2] NIST Special Publication 800-53A, Revision 4, page B-3
[3] NIST Special Publication 800-53A, Revision 4, page B-6

Control Center Ownership

The requirements are very clear about implementing protection for data being used for Operational Planning Analysis, Real-time Assessment, and Real-time monitoring while being transmitted between Control Centers owned by a single Responsible Entity. They also cover the applicable data transmitted between Control Centers owned by two or more separate Responsible Entities. Applying protection among a Responsible Entity's owned Control Centers is solely at its discretion. Applying protection between Control Centers owned by more than one Responsible Entity requires additional diligence. The requirements do not explicitly require formal agreements between Responsible Entities partnering for transmission of applicable data. It is strongly recommended, however, that these partnering entities develop agreements, or use existing ones, to define responsibilities to ensure adequate protection is applied. For example as noted in FERC Order No. 822 Paragraph 59, "if several registered entities have joint responsibility for a cryptographic key management system used between their respective Control Centers, they should have the prerogative to come to a consensus on which organization administers that particular key management system." It is important to note that each Responsible Entity may be held individually accountable for the protection applied to the communications methods of data used for Operational Planning Analysis, Real-time Assessment, and Real-time that is transmitted between Control Centers.

As an example, the reference model below depicts some of the data transmissions between Control Centers that a Responsible Entity should consider to be in-scope. The example does not include all possible scenarios. The green solid lines are in-scope communications. The red dashed lines are out-of-scope communications.



Requirement R2

R2. *The Responsible Entity shall implement the plan(s) specified in Requirement R1, except under CIP Exceptional Circumstances.*

General Considerations for R2

The security objective of Requirement R1 can be achieved through a variety of methods or combinations of methods, such as site to site encryption, application layer encryption, physical protection, etc. The protection must prevent unauthorized disclosure or modification of applicable data on the applicable communication methods between Control Centers identified in 1.1. The Responsible Entity has the discretion to choose and apply protection that meets the security objective.

References

Here are several references to assist entities in developing plan(s) for protection of communication links:

- NIST Special Publication 800-53A, Revision 4: Security and Privacy Controls for Federal Information Systems and Organizations
- NIST Special Publication 800-82: Guide to Industrial Control Systems (ICS) Security
- NIST Special Publication 800-175B: Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms
- NIST Special Publication 800-47: Security Guide for Interconnecting Information Technology Systems

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Comment Form

Project 2016-02 Modifications to CIP Standards
Glossary of Terms Used in NERC Reliability Standards – Control Center

Do not use this form for submitting comments. Use the electronic form to submit comments on **Project 2016-02 Modifications to NERC Glossary of Terms Used in Reliability Standards – Control Center.** The electronic form must be submitted by **8 p.m. Tuesday, September 12, 2017.**

Additional information is available on the project page. If you have questions, contact Standards Developers, Katherine Street (404-446-69702) or Mat Bunch (404-446-9785).

Background Information

The Standard Authorization Request (SAR) of the Project 2016-02 Modifications to CIP Standards Standard Drafting Team (Project 2016-02 SDT) contains multiple issue areas that impact Control Centers. These areas include clarifying applicability for Transmission Owners performing

the functional obligations of Transmission Operators, and protecting communication links and sensitive Bulk Electric System (BES) data communicated between BES Control Centers. In the course of its research of these issues, the SDT has identified potential improvements to the Control Center definition.

In the development of the current Control Center definition, the Project 2008-06 Cyber Security Order 706 Version 5 CIP Standards Standard Drafting Team (Project 2008-06 SDT) received comments[1] stating that the scope of the Control Center definition did not adequately identify control centers. The comment noted that the defined term Control Center could inaccurately apply to some generator plant control rooms. In response, the Project 2008-06 SDT created criteria in CIP-002 that would categorize BES Cyber Systems associated with these facilities as low impact. Since there were no low impact requirements specific to Control Centers, this temporarily mitigated the issue. The Project 2016-02 SDT is now proposing the development of new requirements that apply to low impact Control Centers in its draft CIP-012 standard. The 2016-02 SDT is seeking feedback on whether modifications to the Control Center definition are also necessary.

The SDT is seeking comments on potential modifications to the Control Center definition to provide further clarification of the term "operating personnel." The proposed Control Center definition identifies facilities that have two characteristics. The first characteristic is that the facility hosts operating personnel that perform Real-time reliability-related tasks to operate the Bulk Electric System. The second characteristic is that the facility contains BES Cyber Systems that are used by operating personnel to

[1] *See Consideration of Comments Cyber Security Order 706 Version 5 CIP Standards Comment Form D Definitions and Implementation Plans,* Page 21, available at: http://www.nerc.com/pa/Stand/Project20086CyberSecurityOrder706Version5CIPStanda/Consideration_of_Comments_D_2008-06_091012.pdf. "One commenter suggested that Control Center as it applies to the function of a Generation Operator has a threshold of generation located at two or more locations, and that this single qualifier could unintentionally sweep in the control centers for multi-location generation of very small capacity. The commenter suggested that a capacity qualifier be added to this definition. The SDT does not think that the threshold should be in the definition, but has amended the criterion for generation Control Centers in the Medium Impact category that addresses this comment."

monitor and control the BES. The SDT asserts that operating personnel in this definition should align with personnel already identified in Reliability Standard PER-005-2. The purpose of Reliability Standard PER-005-2 is, "[t]o ensure that personnel performing or supporting Real-time operations on the Bulk Electric System are trained using a systematic approach." The proposed revisions to the Control Center definition clarify that operating personnel perform Real-time reliability-related tasks and lists functional entities that perform those tasks as identified in the applicability section of PER-005-2.

Proposed Definition of "Control Center"

Revised Definition:
One or more facilities, including their associated data centers, that monitor and control the Bulk Electric System (BES) and host operating personnel who perform Real-time reliability-related tasks of: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for Transmission Facilities at two or more locations, or 4) a Generator Operator for generation Facilities at two or more locations.

For Reliability Coordinators, Balancing Authorities, and Transmission Operators, the operating personnel above are System Operators.

For Transmission Owners performing the Real-time reliability-related tasks of a Transmission Operator, the operating personnel above consist of personnel, excluding field switching personnel, who can act independently to operate or direct the operation of the Transmission Owner's Bulk Electric System Transmission Facilities in Real-time.

For Generator Operators, the operating personnel above consist of dispatch personnel at a centrally located dispatch center who receive direction from the Generator Operator's Reliability Coordinator, Balancing Authority, Transmission Operator, or Transmission Owner, and have the capability to develop specific dispatch instructions for plant operators under their control. These personnel do not include plant operators located at a generator plant site or personnel at a centrally located dispatch center who relay dispatch instructions without making any modifications.

Redline Definition:
One or more facilities, including their associated data centers, that monitor and control the Bulk Electric System (BES) and host ~~hosting~~ operating personnel ~~that monitor and control the Bulk Electric System (BES) in real-time to~~ who perform ~~the~~ Real-time reliability-related tasks~~, including their associated data centers,~~ of: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for Transmission Facilities at two or more locations, or 4) a Generator Operator for generation Facilities at two or more locations.

For Reliability Coordinators, Balancing Authorities, and Transmission Operators, the operating personnel above are System Operators.

For Transmission Owners performing the Real-time reliability-related tasks of a Transmission Operator, the operating personnel above consist of personnel, excluding field switching personnel, who can act independently to operate or direct the operation of the Transmission Owner's Bulk Electric System Transmission Facilities in Real-time.

For Generator Operators, the operating personnel above consist of dispatch personnel at a centrally located dispatch center who receive direction from the Generator Operator's Reliability Coordinator, Balancing Authority, Transmission Operator, or Transmission Owner, and have the capability to develop specific dispatch instructions for plant operators under their control. These personnel do not include plant

operators located at a generator plant site or personnel at a centrally located dispatch center who relay dispatch instructions without making any modifications.

Currently Approved Definition:
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, of: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for transmission Facilities at two or more locations, or 4) a Generator Operator for generation Facilities at two or more locations.

Questions

The SDT seeks comment on the potential modifications to the definition of Control Center to clarify the scope of included facilities by identifying the operating personnel at Control Centers performing various registered functions.

1. Control Center definition: The SDT seeks comment on potential modifications to the definition of Control Center to clarify the scope of included facilities by identifying the operating personnel at Control Centers under various functional registrations based on the applicability language in PER-005-2. Do you agree with the alignment to PER-005-2? If not, please provide rationale or propose an alternative definition.

   ☐ Yes
   ☐ No

   Comments:

2. Control Center definition: Do the potential modifications to the Control Center definition change the scope or intent of any current or pending Reliability Standard(s) (examples include Reliability Standards: COM-001-3; TOP-001-4; and IRO-002-5)? If yes, provide details of the affected Reliability Standard(s), requirements, and any anticipated impact.

   ☐ Yes
   ☐ No

   Comments:

3. Control Center definition: The SDT contends that there will be no change in BES Cyber System categorization by clarifying the definition of Control Center. This assertion is based on SDT review of the CIP-002-5.1a criteria and its understanding of BES Cyber System categorization through experience implementing CIP-002-5.1a. Do you agree with this assertion? If not, please provide rationale and practical examples of where a change in categorization will occur as a result of this modification.

   ☐ Yes
   ☐ No

   Comments:

4. Control Center definition: Do you agree with the potential definition of Control Center? If not, please provide rationale or propose an alternative definition.

   ☐ Yes
   ☐ No

   Comments:

5. Implementation Plan: The SDT proposes to make the new Control Center definition effective upon applicable governmental authority's order approving the definition, or as otherwise provided for by the applicable governmental authority. Do you agree with this proposal not to provide additional implementation time following approval? If you agree with the potential implementation time period, please note the actions you will take that require this amount of time to complete. If you think an alternate implementation time period is needed, please propose an alternate implementation period and provide a detailed explanation of actions and time needed to meet your proposed implementation deadline.

   ☐ Yes
   ☐ No

   Comments:

6. If you have additional comments on the proposed definition of Control Center that you have **not** provided in response to the questions above, please provide them here.

   Comments:

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Comment Form

Project 2016-02 Modifications to CIP Standards
Cyber Security – Control Center Communication Networks
Technical Rationale and Justification for CIP-012-1

Do not use this form for submitting comments. Use the electronic form to submit comments on **Project 2016-02 Modifications to CIP Standards CIP-012-1 – Cyber Security – Control Center Communication Networks.** The electronic form must be submitted by **8 p.m. Eastern, Tuesday, September 12, 2017.**

Additional information is available on the project page. If you have questions, contact Standards Developers, Katherine Street (404-446-69702) or Mat Bunch (404-446-9785).

Background Information

On January 21, 2016, the Commission issued Order No. 822, approving seven CIP Reliability Standards and new or modified definitions, and directing modifications to the CIP Reliability Standards. Among others, the Commission directed NERC to "develop modifications to the CIP Reliability Standards to require responsible entities to implement controls to protect, at a minimum, communication links and sensitive bulk electric system data communicated between bulk electric system Control Centers in a manner that is appropriately tailored to address the risks posed to the bulk electric system by the assets being protected (i.e., high, medium, or low impact)." (Order 822, Paragraph 53)

The Project 2016-02 Standard Drafting Team (SDT) drafted Reliability Standard CIP-012-1 to require Responsible Entities to implement controls to protect sensitive Bulk Electric System (BES) data and communications links between BES Control Centers. Due to the sensitivity of the data being communicated between the Control Centers, as defined in the NERC Glossary of Terms Used in Reliability Standards, the standard applies to all impact levels (i.e., high, medium, or low impact).

To complement the requirements drafted in CIP-012-1, the SDT drafted and seeks comment on the Technical Rationale and Justification for CIP-012-1.

Questions

1. The SDT developed draft Technical Rationale and Justification for CIP-012-1 to provide stakeholders and the ERO Enterprise an understanding of the technology and technical requirements in the Reliability Standard. Do you agree that the draft Technical Rationale and Justification for CIP-012-1 clearly explains the technical reasoning for the proposed standard? If you do not agree, or if you agree but have comments or suggestions for the draft document, please provide your recommendation and explanation.

   ☐ Yes
   ☐ No

   Comments:

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2016-02 Modifications to CIP Standards

Informal Comment Period Open through September 12, 2017

Now Available

Two simultaneous 30-day informal comment periods on the **proposed definition of "Control Center"** and the **Technical Rationale and Justification for CIP-012-1 – Cyber Security – Control Center Communication Networks** are open through **8 p.m. Eastern, Tuesday, September 12, 2017**.

Commenting

Use the electronic forms to submit comments. If you experience any difficulties using the electronic forms, contact Wendy Muller. Unofficial Word versions of the comment forms are posted on the project page.

If you are having difficulty accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out, contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern).

- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*
- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Next Steps

The drafting team will review all responses received during the informal comment periods and determine the next steps of the project.

For information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, Katherine Street (via email) or at (404) 446-9702 or Mat Bunch (via email) or at (404) 446-9785.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Comment Report

Project Name:	2016-02 Modifications to CIP Standards | Proposed Definition of Control Center
Comment Period Start Date:	8/14/2017
Comment Period End Date:	9/12/2017
Associated Ballots:	

There were 51 sets of responses, including comments from approximately 181 different people from approximately 119 companies representing 10 of the Industry Segments as shown in the table on the following pages.

Questions

1. Control Center definition: The SDT seeks comment on potential modifications to the definition of Control Center to clarify the scope of included facilities by identifying the operating personnel at Control Centers under various functional registrations based on the applicability language in PER-005-2. Do you agree with the alignment to PER-005-2? If not, please provide rationale or propose an alternative definition.

2. Control Center definition: Do the potential modifications to the Control Center definition change the scope or intent of any current or pending Reliability Standard(s) (examples include Reliability Standards: COM-001-3; TOP-001-4; and IRO-002-5)? If yes, provide details of the affected Reliability Standard(s), requirements, and any anticipated impact.

3. Control Center definition: The SDT contends that there will be no change in BES Cyber System categorization by clarifying the definition of Control Center. This assertion is based on SDT review of the CIP-002-5.1a criteria and its understanding of BES Cyber System categorization through experience implementing CIP-002-5.1a. Do you agree with this assertion? If not, please provide rationale and practical examples of where a change in categorization will occur as a result of this modification.

4. Control Center definition: Do you agree with the potential definition of Control Center? If not, please provide rationale or propose an alternative definition.

5. Implementation Plan: The SDT proposes to make the new Control Center definition effective upon applicable governmental authority's order approving the definition, or as otherwise provided for by the applicable governmental authority. Do you agree with this proposal not to provide additional implementation time following approval? If you agree with the potential implementation time period, please note the actions you will take that require this amount of time to complete. If you think an alternate implementation time period is needed, please propose an alternate implementation period and provide a detailed explanation of actions and time needed to meet your proposed implementation deadline.

6. If you have additional comments on the proposed definition of Control Center that you have not provided in response to the questions above, please provide them here.

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
Southern Company - Southern Company Services, Inc.	Brandon Cain	1,3,5,6	FRCC,MRO,NPCC,SERC,SPP RE,Texas RE,WECC	Southern Company	Katherine Prewitt	Southern Company - Southern Company Services, Inc.	1	SERC
					R. Scott Moore	Southern Company - Alabama Power Company	3	SERC
					William D. Shultz	Southern Company - Southern Company Generation	5	SERC
					Jennifer Sykes	Southern Company - Southern Company Generation and Energy Marketing	6	SERC
Florida Municipal Power Agency	Brandon McCormick	3,4,5	FRCC	FMPA	Tim Beyrle	City of New Smyrna Beach Utilities Commission	4	FRCC
					Jim Howard	Lakeland Electric	5	FRCC
					Lynne Mila	City of Clewiston	4	FRCC
					Javier Cisneros	Fort Pierce Utilities Authority	3	FRCC
					Randy Hahn	Ocala Utility Services	3	FRCC
					Don Cuevas	Beaches Energy Services	1	FRCC
					Jeffrey Partington	Keys Energy Services	4	FRCC
					Tom Reedy	Florida Municipal Power Pool	6	FRCC

					Steven Lancaster	Beaches Energy Services	3	FRCC
					Mike Blough	Kissimmee Utility Authority	5	FRCC
					Chris Adkins	City of Leesburg	3	FRCC
					Ginny Beigel	City of Vero Beach	3	FRCC
Tennessee Valley Authority	Brian Millard	1,3,5,6	SERC	Tennessee Valley Authority	Scott, Howell D.	Tennessee Valley Authority	1	SERC
					Grant, Ian S.	Tennessee Valley Authority	3	SERC
					Thomas, M. Lee	Tennessee Valley Authority	5	SERC
					Parsons, Marjorie S.	Tennessee Valley Authority	6	SERC
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
MRO	Dana Klem	1,2,3,4,5,6	MRO	MRO NSRF	Joseph DePoorter	Madison Gas & Electric	3,4,5,6	MRO
					Larry Heckert	Alliant Energy	4	MRO
					Amy Casucelli	Xcel Energy	1,3,5,6	MRO
					Michael Brytowski	Great River Energy	1,3,5,6	MRO
					Jodi Jensen	Western Area Power Administration	1,6	MRO
					Kayleigh Wilkerson	Lincoln Electric System	1,3,5,6	MRO
					Mahmood Safi	Omaha Public Power District	1,3,5,6	MRO
					Brad Parret	Minnesota Powert	1,5	MRO
					Terry Harbour	MidAmerican Energy Company	1,3	MRO
					Tom Breene	Wisconsin Public Service Corporation	3,5,6	MRO

					Jeremy Voll	Basin Electric Power Cooperative	1	MRO
					Kevin Lyons	Central Iowa Power Cooperative	1	MRO
					Mike Morrow	Midcontinent ISO	2	MRO
Midcontinent ISO, Inc.	David Francis	2,3	FRCC,MRO,NPCC,RF,SERC,SPP RE,Texas RE,WECC	SRC + SWG	Gregory Campoli	New York Independent System Operator	2	NPCC
					Mark Holman	PJM Interconnection, L.L.C.	2	RF
					Charles Yeung	Southwest Power Pool, Inc. (RTO)	2	SPP RE
					Terry BIlke	Midcontinent ISO, Inc.	2	RF
					Elizabeth Axson	Electric Reliability Council of Texas, Inc.	2,3	Texas RE
					Ben Li	IESO	1	MRO
					Drew Bonser	SWG	NA - Not Applicable	NA - Not Applicable
					Darrem Lamb	CAISO	2	WECC
					Matt Goldberg	ISONE	2	NPCC
SERC Reliability Corporation	David Greene	10	SERC	SERC CIPC	Bill Peterson	SERC RRO	10	SERC
					Mike Hagee	SERC RRO	10	SERC
					SERC CIPC	Various	1,2,5,9	SERC
Seattle City Light	Ginette Lacasse	1,3,4,5,6	WECC	Seattle City Light Ballot Body	Pawel Krupa	Seattle City Light	1	WECC
					Hao Li	Seattle City Light	4	WECC
					Bud (Charles) Freeman	Seattle City Light	6	WECC
					Mike Haynes	Seattle City Light	5	WECC
					Michael Watkins	Seattle City Light	1,4	WECC

					Faz Kasraie	Seattle City Light	5	WECC
					John Clark	Seattle City Light	6	WECC
					Tuan Tran	Seattle City Light	3	WECC
					Laurrie Hammack	Seattle City Light	3	WECC
Santee Cooper	James Poston	1,3,5,6		Santee Cooper	Rene' Free	Santee Cooper	1	SERC
					Rodger Blakely	Santee Cooper	1	SERC
					Chris Jimenez	Santee Cooper	1	SERC
					Troy Lee	Santee Cooper	1	SERC
					Tom Abrams	Santee Cooper	1	SERC
					Jennifer Richards	Santee Cooper	1	SERC
					Stony Martin	Santee Cooper	1	SERC
					Glenn Stephens	Santee Cooper	1	SERC
					Tom Perry	Santee Cooper	1	SERC
Entergy	Julie Hall	6		Entergy/NERC Compliance	Oliver Burke	Entergy - Entergy Services, Inc.	1	SERC
					Jaclyn Massey	Entergy - Entergy Services, Inc.	5	SERC
Associated Electric Cooperative, Inc.	Mark Riley	1,3,5,6		AECI & Member G&Ts	Mark Riley	Associated Electric Cooperative, Inc.	1	SERC
					Brian Ackermann	Associated Electric Cooperative, Inc.	6	SERC
					Brad Haralson	Associated Electric Cooperative, Inc.	5	SERC
					Todd Bennett	Associated Electric Cooperative, Inc.	3	SERC
					Michael Bax	Central Electric Power	1	SERC

						Cooperative (Missouri)		
					Adam Weber	Central Electric Power Cooperative (Missouri)	3	SERC
					Ted Hilmes	KAMO Electric Cooperative	3	SERC
					Walter Kenyon	KAMO Electric Cooperative	1	SERC
					Stephen Pogue	M and A Electric Power Cooperative	3	SERC
					William Price	M and A Electric Power Cooperative	1	SERC
					Mark Ramsey	N.W. Electric Power Cooperative, Inc.	1	SERC
					Kevin White	Northeast Missouri Electric Power Cooperative	1	SERC
					Skyler Wiegmann	Northeast Missouri Electric Power Cooperative	3	SERC
					John Stickley	NW Electric Power Cooperative, Inc.	3	SERC
					Jeff Neas	Sho-Me Power Electric Cooperative	3	SERC
					Peter Dawson	Sho-Me Power Electric Cooperative	1	SERC
BC Hydro and Power Authority	Patricia Robertson	1,3,5		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	1,2,3,4,5,6,7,8,9,10	NPCC	RSC no Con-Edison and Dominion	Guy V. Zito	Northeast Power Coordinating Council	10	NPCC
					Randy MacDonald	New Brunswick Power	2	NPCC
					Wayne Sipperly	New York Power Authority	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	Orange & Rockland Utilities	3	NPCC
					Michele Tondalo	UI	1	NPCC
					Laura Mcleod	NB Power	1	NPCC
					Michael Schiavone	National Grid	1	NPCC
					Michael Jones	National Grid	3	NPCC
					David Ramkalawan	Ontario Power Generation Inc.	5	NPCC
					Quintin Lee	Eversource Energy	1	NPCC
					Kathleen Goodman	ISO-NE	2	NPCC
					Greg Campoli	NYISO	2	NPCC
					Silvia Mitchell	NextEra Energy - Florida Power and Light Co.	6	NPCC
					Paul Malozewski	Hydro One Networks, Inc.	3	NPCC
					Sylvain Clermont	Hydro Quebec	1	NPCC
					Helen Lainis	IESO	2	NPCC
					Chantal Mazza	Hydro Quebec	2	NPCC

Dominion - Dominion Resources, Inc.	Sean Bodkin	3,5,6		Dominion	Connie Lowe	Dominion - Dominion Resources, Inc.	3	NA - Not Applicable
					Lou Oberski	Dominion - Dominion Resources, Inc.	5	NA - Not Applicable
					Larry Nash	Dominion - Dominion Virginia Power	1	NA - Not Applicable
Southwest Power Pool, Inc. (RTO)	Shannon Mickens	2	SPP RE	SPP Standards Review Group	Shannon Mickens	Southwest Power Pool Inc.	2	SPP RE
					Deborah McEndaffer	Midwest Energy, Inc.	NA - Not Applicable	SPP RE
					Don Schmit	Nebraska Public Power District	5	SPP RE
					Louis Guidry	Cleco Corporation	1,3,5,6	SPP RE
					Robert Hirchak	Cleco Corporation	6	SPP RE
					Marty Paulk	Cleco Corporation	1,3,5,6	SPP RE
					Michelle Corley	Cleco Corporation	3	SPP RE
					Robert Gray	Board of Public Utilities	NA - Not Applicable	SPP RE
					Ron Spicer	EDP Renewables	NA - Not Applicable	SPP RE
					Steven Keller	Southwest Power Pool	2	SPP RE
					Laura Cox	Westar Energy	5	SPP RE
PPL - Louisville Gas and Electric Co.	Shelby Wade	3,5,6	RF,SERC	Louisville Gas and Electric Company and Kentucky Utilities Company	Charles Freibert	PPL - Louisville Gas and Electric Co.	3	SERC
					Dan Wilson	PPL - Louisville Gas and Electric Co.	5	SERC
					Linn Oelker	PPL - Louisville Gas and Electric Co.	6	SERC
PSEG	Sheranee Nedd	1,3,5,6	NPCC,RF	PSEG REs	Tim Kucey	PSEG - PSEG Fossil LLC	5	RF
					Karla Jara	PSEG Energy Resources and Trade LLC	6	RF

					Jeffrey Mueller	PSEG - Public Service Electric and Gas Co	3	RF
					Joseph Smith	PSEG - Public Service Electric and Gas Co	1	RF

1. Control Center definition: The SDT seeks comment on potential modifications to the definition of Control Center to clarify the scope of included facilities by identifying the operating personnel at Control Centers under various functional registrations based on the applicability language in PER-005-2. Do you agree with the alignment to PER-005-2? If not, please provide rationale or propose an alternative definition.

Matthew Beilfuss - WEC Energy Group, Inc. - 3,4,5,6 - MRO,RF

Answer	No
Document Name	

Comment

PER-005-2 does not use Real-time reliability related tasks when referring to a GOP. The proposed definition implies these tasks exist. A GOP does not perform a Real-time reliability related task. Therefore, no GOP would have a Control Center that meets the definition.

Likes 0	
Dislikes 0	

Response

George Brown - Acciona Energy North America - 5

Answer	No
Document Name	

Comment

The Control Center definition should only define a physical location where Real-time Bulk Electrical System (BES) reliability related operating tasks are performed. It also can include, but cautiously, information on personnel that a Control Center houses, however it should not attempt to define these personnel, either System Operators or operating personnel.

If it is the intention of the SDT to define operating personnel of a Transmission Owner (TO) performing the Real-time reliability-related operating tasks of a Transmission Operator and Generator Operator (GOP) operating personnel, then a separate term needs to be defined to identify these individuals.

Data centers usually do not host personnel and the proposed Control Center definition needs to be modified to account for this.

In the context of the proposed definition of Control Center, in the Generator Operator section, the term “direction” is used, “Operating Instruction” is already a defined term and should be used instead of “direction”. Also, the term “capability” is used and is inaccurate, many individuals have the capability to modify a generator, i.e. IT/OT personnel, however, few have the authority; “capability should be modified to “authority”.

The following is suggested:

Control Center: One or more facilities that monitor and control the Bulk Electric System and host System Operators and Operating Personnel who perform the Real-time operating reliability related-tasks, and includes the associated data centers, of:

1) a Reliability Coordinator,

2) a Balancing Authority,

3) a Transmission Operator for Transmission Facilities at two or more locations,

4) a Transmission Owner performing the delegated Real-time reliability-related operating tasks of a Transmission Operator at two or more locations or

5) a Generator Operator for generation Facilities at two or more locations.

Operating Personnel: An individual at a Control Center of a Transmission Owner or Generator Operator who perform the Real-time operating reliability related-tasks as follows:

1. For a Transmission Owner these individuals would be personnel who can act independently and have the authority to operate or direct the operation of the Transmission Owner's Bulk Electric System Transmission Facilities in Real-time.

2. For a Generator Operator these individuals would be personnel who receive Operating Instructions from the Generator Operator's Reliability Coordinator, Balancing Authority, Transmission Operator, or Transmission Owner, and have the authority to develop and direct specific dispatch instructions for plant operators under their control. These personnel do not include plant operators located at a generator plant site or personnel at a centrally located dispatch center who relay Operating Instructions and dispatch instructions without making any modifications.

Likes 0	
Dislikes 0	

Response

Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	No
Document Name	

Comment

The NSRF has great concerns with the wording of "...having the capability…" This wording is ambiguous since everyone has the "capability" to do develop dispatch instructions even if they are not authorized to do so. Recommend that "having the capability" be changed to "have the authority". This clearly states that the GOP can make said adjustments.

For Generator Operators, the operating personnel above consist of dispatch personnel at a centrally located dispatch center who receive direction from the Generator Operator's Reliability Coordinator, Balancing Authority, Transmission Operator, or Transmission Owner, and **have the capability** to develop specific dispatch instructions for plant operators under their control. This personnel does not include plant operators located at a generator plant site or personnel at a centrally located dispatch center who relay dispatch instructions without making any modifications.

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	No
Document Name	

Comment

Texas RE appreciates the Standard Drafting Team's (SDT) effort to clarify the Control Center definition within the overall project scope set forth in the governing Standards Authorization Request (SAR). While Texas RE does not necessarily object to these clarifications and understands that the SDT's intent is not to substantively alter the Control Center definition as it is currently applied to registered entities, Texas RE is concerned that the overall project may increase confusion around the application of the Control Center definition across the industry.

As an initial matter, Texas RE notes that there are a number of areas in which there is a clear need for further clarity regarding the use of the term "Control Center." Texas RE has identified several standards using descriptors such as primary and backup, several standards where the term control center is not capitalized, and standards with confusion regarding the TO acting as TOP. Texas RE respectfully requests that the SDT consider these additional applications and scenarios as part of a more comprehensive review of the "Control Center" definition.

For example, EOP-008 refers to functionality at an entity's "primary control center" and "backup control center." In either case, the term "control center" is not capitalized and therefore does not appear to refer to the defined term. In contrast, IRO-002-5 R2 and R3, in parallel with TOP-001-4 R23 and 24 reference "primary Control Centers." Here, the reference is to the defined "Control Center" term, but there is no defined understanding in the standards of what constitutes a primary Control Center. It seems that the new definition removes the need for descriptors such as "primary" and "back up".

The following standards use the term control center, which is not capitalized: BAL-005-0.2b, BAL-006-2, CIP-014-2, COM-001-3, EOP-008-1, EOP-008-2, and FAC-003-4.

Texas RE is supportive of a more narrowly focused effort to correct the obvious NERC Registration issues with the "TO acting as a TOP" issue. Most importantly, TOP is a certified function and the fact that TOs are acting as a TOP without the requisite certification is a potential reliability gap that should be taken more seriously by the ERO. The following Standards/Requirements do not adequately cover TOs acting as a TOP:

- COM-001-3 R12: Field personnel are called out for having communication capability but are excluded in the definition of Control Center. This will create confusion and inconsistent implementation of applicability.
- IRO-002-5 R2: TOs acting as TOPs may be considered only if the RC "deems necessary". It is apparent that the establishment of compliance obligations that are contingent on non-definitive terms such as "deems necessary" with no specificity or criteria do not occur in a consistent manner. This leads to poor communication and reliability gaps due to compliance concerns (or compliance postures where a company, in this example an RC, does not want to place a compliance burden on a company due to the political nature of such an act).
- CIP-014-2 in its entirety missed a "TO acting as a TOP" partially because that condition is not fully recognized and the term "Control Center" is lower cased. Does the SDT believe there is a difference between the proposed definition and the lower-case term? If so, what is it?

Beyond these scoping issues, Texas RE is concerned that the proposed clarifications may inadvertently introduce more ambiguity into the Standard in two areas. First, the "Control Center" definition continues to hinge on the concept of a facility that "hosts" operating personnel. Texas RE has consistently interpreted this language to describe the intended functionality of a facility and not to imply any current staffing levels or operations. That is to say, the fact that a Control Center operating as an entity's backup facility is not currently hosting operating personnel does not mean that facility is not a "Control Center" under the definition. Although the proposed revisions do not appear intended to alter this common sense interpretation, the introduction of the conjunctive "and" could possibly lead entities to conclude that until a Control Center is actually hosting operating personnel, the mere fact that it can monitor and control the Bulk Electric System does not render that facility a "Control Center" as defined. Texas RE requests that the SDT clarify that facilities that have the purpose of hosting operating personnel are subject to the Control Center definition, regardless of whether they have done so or not.

Second, Texas RE notes that the proposed “Control Center” definition could be interpreted to limit Generator Operator “Control Centers” subject to the definition. In particular, the SDT has elected to fold training requirements for Generator Operator personnel into the Control Center definition, presumably to provide clarity around the scope of facilities that “host operating personnel.” Texas RE noticed the proposed description of GOP operating personnel utilizes the description of dispatch personnel in PER-005-2. Texas RE requests the SDT evaluate the tasks for each dispatch personnel and operating personnel to determine whether or not this is appropriate. Folding this training requirement directly into the Control Center definition may result in further confusion. In Texas RE’s experience, numerous GOPs have the capability to develop dispatch instructions and may take various actions in response to requests from their Reliability Coordinators or Transmission Operators, including altering their voltage profile or Real power output. It is not clear in what circumstances these constitute “developing dispatch instructions.” A better approach may be to clarify that operating personnel include persons that “are capable of developing dispatch instructions” to reduce ambiguity about the scope of the Control Center definition as it pertains to the internal operating procedures of specific Generator Operators.

Likes 0	
Dislikes 0	

Response

Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body

Answer	No
Document Name	

Comment

SCL supports the APPA submitted comments.

Likes 0	
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion

Answer	No
Document Name	

Comment

Dominion generally agrees with the alignment to PER-005-2. Dominion has concerns that one of the requirements of PER-005-2 is to “create a list of BES company-specific Real-time reliability-related tasks based on a defined and documented methodology”. This clause results in the proposed definition being dependent on the execution of PER-005-2, and can vary from one Entity to another. Also, the phrase “Real-time reliability-related tasks” is not specifically used in reference to Generator Operators in PER-005-2.

Dominion suggests the following changes to the proposed defintion to resolve this issue:

One or more facilities, including their associated data centers, of an RC, BA, TOP, TO, GOP that monitor and control the Bulk Electric System (BES) and host operating personnel who perform Real-time reliability-related tasks of: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for Transmission Facilities at two or more locations, or 4) a Generator Operator for generation Facilities at two or more locations.have the

capability to operate or direct in Real-time the operation of Bulk Electric System Transmission Facilities at two or more locations or have the capability to direct specific dispatch instructions to plant operators or plant control systems for generation Facilities at two or more locations.

Likes 0	
Dislikes 0	

Response

Thomas Breene - WEC Energy Group, Inc. - 3,4,5,6

Answer	No
Document Name	

Comment

We have great concerns with the wording of "...having the capability…". This wording is ambiguous since everyone has the "capability" to do develop dispatch instructions even if they are not authorized to do so. Recommend that "having the capability" be changed to "have the authority". This clearly states that the GOP can make said adjustments.

For Generator Operators, the operating personnel above consist of dispatch personnel at a centrally located dispatch center who receive direction from the Generator Operator's Reliability Coordinator, Balancing Authority, Transmission Operator, or Transmission Owner, and **have the capability** to develop specific dispatch instructions for plant operators under their control. These personnel do not include plant operators located at a generator plant site or personnel at a centrally located dispatch center who relay dispatch instructions without making any modifications.

While including personnel roles executed helps to clarify what is and what isn't a Control Center, the definitions of those roles should be standalone in the NERC Glossary of Terms. I.E. "Operating Personnel" should have its own definition and be used as a defined term in the Control Center definition.

Likes 0	
Dislikes 0	

Response

sean erickson - Western Area Power Administration - 1,6

Answer	No
Document Name	

Comment

Per the NSRF: the proposed definition of Control Center. The largest issue is the last paragraph concerning a Generating Operator. The use of the word "capability" is ambiguous and will confuse Registered Entities and CEAs, a like. The SDT should consider the approved Applicability within PER-005-2 part 4.1.5.1, which reads:

Dispatch personnel at a centrally located dispatch center who receive direction from the Generator Operator's Reliability Coordinator, Balancing Authority, Transmission Operator, or Transmission Owner, and may develop specific dispatch instructions for plant operators under their control. These

personnel do not include plant operators located at a generator plant site or personnel at a centrally located dispatch center who relay dispatch instructions without making any modifications.

This aligns with current and understood wording of PER-005-2.

Are the noted “Real-time reliability related- tasks” within the proposed definition, the same “Real-time Reliability-related task prescribed in PER-005-2? If so, please state this in your consideration of comments document and within your guidance document.

Likes 0	
Dislikes 0	

Response

David Francis - Midcontinent ISO, Inc. - 2,3 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG

Answer	No
Document Name	

Comment

The SRC & ITC SWG agrees with the creation of a new standard, rather than expanding CIP-003, CIP-005 and/or CIP-006 requirements to provide new controls over physical communication links. Specifically, the SRC & ITC SWG commends the SDT for recognizing that not all utilities own or control their own physical communications links.

The SRC & ITC SWG offers the following comments and recommendations.

R1. For data used for Operational Planning Analysis, Real-time Assessments, and Real-time monitoring, as documented by a Reliability Coordinator, Transmission Operator, or Balancing Authority, the Responsible Entity shall develop one or more documented plan(s) to mitigate the risk of the unauthorized disclosure or modification of the data while it is being transmitted between Control Centers. This excludes oral communications, regardless of transport means.

The note to R1 concerning the existence of a Control Center or specified data should be a dealt with in Section 4 – Applicability part of the Standard. This would eliminate the need for this to be discussed as part of the RSAW.

Recommend that it be clarified whether this is a standalone Standard similar to CIP-014 or if it is intended to define the scope of applicable systems to be protected under CIP-003 thru CIP-011.

In order to evaluate the extent and kind of obligation involved, the definition of between control centers needs to be clearer with regard to the communication link. The Standard should address the proper demarcation points for obligation to show implementation and compliance. To clearly define the obligation of Responsible Entities, the required plan should include identification of the demarcation points. Information is also needed on the explicit agreements required on each end of the physical communication link to arrange and identify such demarcation. Where there is disagreement on how protections are to be applied between two or more Responsible Entities, what is the arbitration process to resolve these disagreements?

How is the situation handled where a Responsible Entity (e.g., an RC) is receiving information from a third-party provider that is aggregating and submitting data on behalf of one or more Responsible Entities (e.g., a TOP)? What is the identification of the demarcation points? In reading the standard, it does not appear that the connection to the third-party provider is in scope since they are not a Responsible Entity or even registered with NERC. The same situation may be present for entities that use an outsourced data center provider. The question is also relevant for the data that is provided to regulatory agencies that are not bound by CIP Standards.

Likes 0	
Dislikes 0	

Response

Sheranee Nedd - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs

Answer	No
Document Name	

Comment

The definition is not consistent with PER-005-2 part 4.1.5.1. It uses the statement "*have the capability to* develop specific dispatch instructions… ", where PER-005-2 part 4.1.5.1. states "*may* develop specific dispatch instructions…". There is significant difference between having the capability to do something, versus doing it. The language (i.e."may" versus "having the capability to") concerning Generation and Control Centers (a "centrally located dispatch center" in PER-005-2 part 4.1.5.1) has already been settled by industry, through development and approval of PER-005-2. The proposed definition should stay consistent with PER-005-2 part 4.1.5.1.

Likes 3	PSEG - PSEG Fossil LLC, 5, Kucey Tim; PSEG - Public Service Electric and Gas Co., 1, Smith Joseph; PSEG - Public Service Electric and Gas Co., 3, Mueller Jeffrey
Dislikes 0	

Response

Jamie Monette - Allete - Minnesota Power, Inc. - 1

Answer	No
Document Name	

Comment

MP agrees with the NATF's concerns with the wording of "...having the capability…". This wording is ambiguous since everyone has the "capability" to do develop dispatch instructions even if they are not authorized to do so. Recommend that "having the capability" be changed to "have the authority". This clearly states that the GOP can make said adjustments.

For Generator Operators, the operating personnel above consist of dispatch personnel at a centrally located dispatch center who receive direction from the Generator Operator's Reliability Coordinator, Balancing Authority, Transmission Operator, or Transmission Owner, and **have the capability** to

develop specific dispatch instructions for plant operators under their control. These personnel do not include plant operators located at a generator plant site or personnel at a centrally located dispatch center who relay dispatch instructions without making any modifications.

Likes 0	
Dislikes 0	

Response

Barry Lawson - National Rural Electric Cooperative Association - 3,4

Answer	No
Document Name	

Comment

NRECA requests additional clarity to be added to the draft revised Control Center definition. Specifically, in the third paragraph, second and third line, of the definition, replace “who can act independently to operate …..” with “who have independent authority to operate ……” This better and more clearly addresses the capability and independent authority issues.

Likes 0	
Dislikes 0	

Response

David Jendras - Ameren - Ameren Services - 1,3,6

Answer	No
Document Name	

Comment

While the inclusion of the language to link the duties to PER-005 make sense, PER-005 also includes Transmission Owner employees who operate local **control centers.** If the logic holds that PER-005 attributes are linked to these requirements, we believe the omission of Transmission Owners is inappropriate. Even though Transmission Owners are discussed in the third paragraph, they should be listed as number 5) to ensure TO personnel hosted at such a facility would qualify that facility.

Likes 0	
Dislikes 0	

Response

Brandon Cain - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE, Group Name Southern Company

Answer	No
Document Name	
Comment	
Southern respectfully disagrees with the approach used by the SDT to re-define the term Control Center based solely on the functions of a facility's operating personnel (as defined in PER-005-2) rather than based on the reliability impact of the equipment and data associated with the facility. We believe the proposed definition may result in the unintended consequence of omitting dispatch centers with control over significant amounts of generation because operating personnel in the facility do not modify dispatch instructions they receive from their RC, BA or TOP.	
Likes 0	
Dislikes 0	
Response	

Annette Johnston - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3

Answer	No
Document Name	
Comment	
We agree with the concept of aligning with PER-005-2 with two exceptions. First, the existing language for PER-005-2 has become somewhat outdated because it does not comprehend renewable energy such as wind and solar. A wind farm is not a plant site, but personnel for a wind farm should be excluded too. Second, the language for generator operator was changed from "may develop" to "have the capability to develop." Consider, "and develops".	
Likes 0	
Dislikes 0	
Response	

Brandon McCormick - Florida Municipal Power Agency - 3,4,5 - FRCC, Group Name FMPA

Answer	Yes
Document Name	
Comment	
Agree with the alignment but not the specific wording Request clarification of the Transmission Owner's "field switching personnel," for this definition. This term was not explained well in PER-005.	

Request clarification of the Generation Operator – “have the capability to develop specific dispatch instructions.” Should this be the capability to issue instead of capability to develop? The word “capability” is too generic. Suggest that the phrase be changed to “authority to develop or modify the specific dispatch instructions” since authority is related to the generator operating personnel and not the control systems.

Suggest that the phrase “These personnel do not include plant operators located at a generator plant site or personnel at a centrally located dispatch center who relay dispatch instructions without making any modifications.” Be modified to “These personnel do not include plant operators located at a generator plant site or personnel at a centrally located dispatch center who relay verbal dispatch instructions without making any modifications.” This would clarify that this is related to the generator operating personnel and not the

Likes 0	
Dislikes 0	

Response

Marty Hostler - Northern California Power Agency - 5,6

Answer	Yes
Document Name	

Comment

1. NCPA agrees with the SDT decision to align the operating personnel in the Project 2016-02 Standard with personnel identified in Reliability Standard PER-005-2. While the alignment is appropriate, NCPA believes that some wording needs to be clarified.

2. The term, “field switching personnel,” used in the draft control center definition, is not well explained in PER-005-2. Therefore, this term needs to be clarified for use in the CIP Standards.

3. NCPA requests clarification regarding the language associated with Generation Operator (GOP) – that the GOP, “have the capability to develop specific dispatch instructions.” Specifically, is “capability” referring to the capability to issue instructions, or is it the capability to develop instructions? The use of the word “capability” here is too generic and NCPA suggests changing it to, “authority to develop or modify the specific dispatch instructions,” since authority is related to the generator operating personnel and not the control systems.

4. NCPA requests that the phrase, “These personnel do not include plant operators located at a generator plant site, or personnel at a centrally located dispatch center who relay dispatch instructions without making any modifications,” be changed to “These personnel do not include plant operators located at a generator plant site, or personnel at a centrally located dispatch center who relay verbal dispatch instructions without making any modifications.” This would clarify that this is related to the generator operating personnel and not the control systems.

Likes 0	
Dislikes 0	

Response

Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6

Answer	Yes
Document Name	
Comment	

To better ensure alignment with PER-005-2, AZPS suggests clarifying the term Real-time reliability-related tasks as utilized in the definition. An amendment to the first sentence of the definition similar to the following is recommended:

One or more facilities, including their associated data centers, that monitor and control the Bulk Electric System (BES) and host operating personnel who perform Real-time reliability-related tasks ***identified by the Responsible Entity as part of its systematic approach to training under the Operations Personnel Training standard,*** *of: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for Transmission Facilities at two or more locations, or 4) a Generator Operator for generation Facilities at two or more locations.*

An additional possible revision could be:

One or more facilities, including their associated data centers, that monitor and control the Bulk Electric System (BES) and host operating personnel who perform Real-time reliability-related tasks of: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for Transmission Facilities at two or more locations, or 4) a Generator Operator for generation Facilities at two or more locations. Real-time reliability-related tasks are those tasks identified by the Responsible Entity as part of its systematic approach to training under the Operations Personnel Training standard.

Alternatively, AZPS suggests that the SDT define “Real-time reliability-related tasks” in the glossary of terms.

Likes 0	
Dislikes 0	
Response	

Aaron Austin - AEP - 3,5

Answer	Yes
Document Name	
Comment	

AEP suggests the SDT should consider making the argument that the Real-time Reliability Tasks that the personnel and Cyber Assets can perform comprise the rationale for making the change.

Likes 0	
Dislikes 0	
Response	

Russell Noble - Cowlitz County PUD - 3,5

Answer	Yes
Document Name	

Comment
Public Utility District No. 1 of Cowlitz County (District) supports APPA comments. In addition, the District believes the intent is to exclude personnel having no system wide awareness and who manually operate BES Facilities on location, while including personnel who perform autonomous (“independent”) centralized reliability monitoring and remote control (via “Real-time” SCADA) for two or more discrete Transmission Facilities located at unique addresses on ***behalf*** of a registered TOP. While the District agrees with basing operating personnel qualification on the applicability language in PER-005-2 in part, it is not clear if a Control Center is inclusive of a room containing dispatch personnel who can only perform *local reliability* operations which do not impact or concern the covering Transmission Operator’s greater system. The District seeks greater clarification. In particular, it is not clear if autonomous directives related to public safety or quality of service, such as clearing transmission segments compromised by weather or traffic accidents, are inclusive within the undefined term “reliability.” Further, it is not clear what operational aspect of a Transmission Owner’s central control room raises it to the status of a Control Center; note that PER-005-2 avoids associating a TO with a Control Center and performing “tasks of a Transmission Operator.” In the case of the “TO Control Center,” it appears the intent is to limit inclusion to those control rooms containing personnel tasked by the registered TOP to autonomously address events meeting a list of PER-005-2 “BES company-specific Real-time reliability-related” tasks that align with the covering TOP’s Reliable Operation obligation. This will depend on how the TO defines a “BES company-specific Real-time reliability-related task,” and assuming Enforcement agrees. If Enforcement finds the entity in violation of PER-005-2 Requirement R2, this may create double jeopardy with the CIP standards. However, the intent could conversely imply the inclusion of control rooms that have the ability (sans authority) to independently impact the covering TOP’s obligation to Reliably Operate the BES. The District requests the SDT clarify the intent, and submits a possible solution in question 4.

Likes 0	
Dislikes 0	

Response

Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	

Comment
ERCOT ISO supports the comments of the ITC SWG.

Likes 0	
Dislikes 0	

Response

Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes
Document Name	

Comment

Request clarification of the Transmission Owner's "field switching personnel," for this definition. This term was not explained well in PER-005.

Request clarification of the Generation Operator – "have the capability to develop specific dispatch instructions." Should this be the capability to issue instead of capability to develop? The word "capability" is too generic. Suggest that the phrase be changed to "authority to develop or modify the specific dispatch instructions" since authority is related to the generator operating personnel and not the control systems.

Suggest that the phrase "These personnel do not include plant operators located at a generator plant site or personnel at a centrally located dispatch center who relay dispatch instructions without making any modifications." Be modified to "These personnel do not include plant operators located at a generator plant site or personnel at a centrally located dispatch center who relay verbal dispatch instructions without making any modifications." This would clarify that this is related to the generator operating personnel and not the control systems

Likes 0	
Dislikes 0	

Response

Wendy Center - U.S. Bureau of Reclamation - 1,5

Answer	Yes
Document Name	

Comment

Reclamation supports having the Control Center definition only in the Glossary, rather than contained within other standards.

Likes 0	
Dislikes 0	

Response

David Ramkalawan - Ontario Power Generation Inc. - 5

Answer	Yes
Document Name	

Comment

OPG recommend to change the "capability to develop specific dispatch instructions" to "capability to originate or modify and issue specific dispatch instructions".

Likes 0	
Dislikes 0	

Response

Normande Bouffard - Hydro-Qu?bec Production - 1,5	
Answer	Yes
Document Name	

Comment
Alternative proposition for GOP: For Generator Operators, the operating personnel above consist of dispatch personnel at a centrally located dispatch center who receive direction from the Generator Operator's Reliability Coordinator, Balancing Authority, Transmission Operator, or Transmission Owner. These operating personnel only include personnel who can act independently to operate or direct the operation of the Generator Owner's Bulk Electric System Facilities in Real-time.

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Con-Edison and Dominion	
Answer	Yes
Document Name	

Comment
Agree with the alignment but not the specific wording This definition of uses the NERC defined term "System Operator". In the NERC Glossary, the "System Operator" definition uses the term "Control Center." Request this dependency be addressed. Request clarification of the Transmission Owner's "field switching personnel," for this definition. This term was not explained well in PER-005. Request clarification of "who can act independently to operate or direct the operation." Is this addressing capability or authority? Request clarification of the Generation Operator – "have the capability to develop specific dispatch instructions." Should this be the capability to issue instead of capability to develop?

Likes 0	
Dislikes 0	

Response

Lona Calderon - Salt River Project - 1,3,5,6 - WECC

Answer	Yes
Document Name	

Comment

SRP agrees with the alignment of the Control Center definition with PER-005-2, such as the incorporation of the phrase “Real-time reliability related tasks."

Likes 0	
Dislikes 0	

Response

Jack Cashin - American Public Power Association - 4

Answer	Yes
Document Name	

Comment

APPA agrees with the SDT decision to align the operating personnel in the Project 2016-02 Standard with the personnel identified in Reliability Standard PER-005-2. While the alignment is appropriate, public power believes that some of the wording needs clarification.

The term, “field switching personnel,” used in the draft control center definition, is not well explained in PER-005-2. Therefore, this term will need to be clarified for use in the CIP Standards. Specifically, regarding Transmission Owners’ field switching personnel, the term needs clarification to be used effectively in the CIP standards.

Public power agrees with the comments of the Public Utility District No. 1 of Cowlitz County that, while alignment with PER-005-2 is appropriate for Project 2016-02, further clarity is needed regarding personnel roles. Specifically, it should be made clear that the CIP standard’s intent is to exclude personnel having no system-wide awareness and who manually operate BES facilities on location, while including personnel who perform autonomous reliability monitoring and remote control for a registered Transmission Operator (TOP). Further clarity is needed because, under PER-005-2, it is not clear if Control Center personnel include dispatch personnel who only perform local reliability functions rather than impacting the TOP’s greater system. Therefore, while the alignment with PER-005-2 is appropriate, further clarity is needed to work within the CIP standards and prevent significantly changing BES Cyber System categorization (see question 3).

Additionally, public power requests clarification regarding the language associated with Generation Operator (GOP) – that the GOP, “have the capability to develop specific dispatch instructions.” Specifically, is “capability” referring to the capability to issue instructions, or is it the capability to develop instructions? The use of the word “capability” here is too generic and public power suggests changing it to, “authority to develop or modify the specific dispatch instructions,” since authority is related to the generator operating personnel and not the control systems.

APPA also suggests that the phrase, “These personnel do not include plant operators located at a generator plant site, or personnel at a centrally located dispatch center who relay dispatch instructions without making any modifications,” be changed to “These personnel do not include plant operators located at a generator plant site, or personnel at a centrally located dispatch center who relay verbal dispatch instructions without making any modifications.” This would clarify that this is related to the generator operating personnel and not the control systems.

Likes 0	
Dislikes 0	

Response

Mark Riley - Associated Electric Cooperative, Inc. - 1,3,5,6, Group Name AECI & Member G&Ts

Answer	Yes
Document Name	

Comment

AECI supports the SDT's approach to align the Control Center definition with PER-005-2. However, AECI requests additional clarity to be added to the draft Control Center definition. Specifically, in the third paragraph, second and third line, of the definition, replace “who can act independently to operate …..” with “who have independent authority to operate ……”

Likes 0	
Dislikes 0	

Response

Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6

Answer	Yes
Document Name	

Comment

Tacoma Power supports the comments of APPA.

Likes 0	
Dislikes 0	

Response

Nicholas Lauriat - Network and Security Technologies - 1

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	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Chris Scanlon - Exelon - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Poston - Santee Cooper - 1,3,5,6, Group Name Santee Cooper	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Folz - Southern Indiana Gas and Electric Co. - 1,3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Shelby Wade - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Theresa Rakowsky - Puget Sound Energy, Inc. - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Greene - SERC Reliability Corporation - 10, Group Name SERC CIPC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Harold Sherrill - Sempra - San Diego Gas and Electric - 7 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Robert Blackney - Edison International - Southern California Edison Company - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	Yes
Document Name	
Comment	

Likes 1	Stephanie Burns, N/A, Burns Stephanie
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Robertson - BC Hydro and Power Authority - 1,3,5, Group Name BC Hydro	
Answer	Yes
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	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	
Document Name	
Comment	
The California ISO supports the comments of the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	

2. Control Center definition: Do the potential modifications to the Control Center definition change the scope or intent of any current or pending Reliability Standard(s) (examples include Reliability Standards: COM-001-3; TOP-001-4; and IRO-002-5)? If yes, provide details of the affected Reliability Standard(s), requirements, and any anticipated impact.

Brandon Cain - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE, Group Name Southern Company

Answer	No
Document Name	

Comment

Considering the definition's proposed alignment with PER-005, Southern does not see a change in the GOP function based on this definition.

Likes 0	
Dislikes 0	

Response

Lona Calderon - Salt River Project - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

Neither the definition of Control Center proposed by the SDT, nor the definition proposed by SRP in comment #4 affect the scope or intent of any O&P requirements.

SRP agrees with APPA and LPPC that this commenting should not be included along with comments to CIP standards. By doing so, the personnel working exclusively with 693 standards are being excluded and may cause unintentional consequences.

Likes 0	
Dislikes 0	

Response

Wendy Center - U.S. Bureau of Reclamation - 1,5

Answer	No
Document Name	

Comment

Reclamation supports having the Control Center definition only in the Glossary, rather than contained within different standards.	
Likes 0	
Dislikes 0	
Response	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
ERCOT ISO supports the comments of the ITC SWG.	
Likes 0	
Dislikes 0	
Response	
Russell Noble - Cowlitz County PUD - 3,5	
Answer	No
Document Name	
Comment	
The District finds the proposed definition as it relates to the registered functions of the RC, BA, TOP, and GOP does not change the original intent and scope. Further, the proposed definition clarifies “operating personnel” for the RC, BA, and TOP registered functions as System Operators, who are presumably NERC certified (please see question 4). The District strongly agrees with subjecting registered entities with monitoring and enforcement action as officially registered, and seeks full retirement of the phrase “performing the functional obligations of.” Rather, the new definition seeks to define TO activities that closely aligns with certain standard requirements placed on the TOP. The District believes the registered TOP may delegate certain tasks to the TO, but not transfer responsibility. In this case, where the TO is performing Real-time reliability-related tasks – regardless if autonomous or directed – as defined by “Reliable Operation of the BES” on behalf of its TOP, the term Control Center definitely applies. Although the District advances improvements in the definition of Control Center, the District fully supports SDT’s definition modification efforts.	
Likes 0	
Dislikes 0	
Response	
Marty Hostler - Northern California Power Agency - 5,6	
Answer	No

Document Name	
Comment	
CIP standards typically garner comments from information technology personnel rather than from system operations personnel. This could result in the unintended consequence of potential operational impacts not being appropriately identified during the standard balloting and commenting process.	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	No
Document Name	
Comment	
SCL supports the APPA submitted comments.	
Likes 0	
Dislikes 0	
Response	
Matthew Beilfuss - WEC Energy Group, Inc. - 3,4,5,6 - MRO,RF	
Answer	No
Document Name	
Comment	
Though the proposed modifciation (adding transmission owner) has the potential to impact how other standards (EOP-004, EOP-008) consider using the NERC defined term in the future.	
Likes 0	
Dislikes 0	
Response	
Mark Riley - Associated Electric Cooperative, Inc. - 1,3,5,6, Group Name AECI & Member G&Ts	
Answer	No
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jack Cashin - American Public Power Association - 4	
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	

Patricia Robertson - BC Hydro and Power Authority - 1,3,5, Group Name BC Hydro	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Normande Bouffard - Hydro-Qu?bec Production - 1,5	
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	
David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	No
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	No
Document Name	
Comment	
Likes 1	Stephanie Burns, N/A, Burns Stephanie
Dislikes 0	
Response	
Robert Blackney - Edison International - Southern California Edison Company - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Harold Sherrill - Sempra - San Diego Gas and Electric - 7 - WECC	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Greene - SERC Reliability Corporation - 10, Group Name SERC CIPC	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Theresa Rakowsky - Puget Sound Energy, Inc. - 1,3,5	
Answer	No
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Shelby Wade - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Austin - AEP - 3,5	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Amy Folz - Southern Indiana Gas and Electric Co. - 1,3,5,6 - RF	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1,3,5,6	
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	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Annette Johnston - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3	
Answer	Yes
Document Name	
Comment	
The change in the definition could impact CIP-012 scope.	
Likes 0	
Dislikes 0	
Response	

David Jendras - Ameren - Ameren Services - 1,3,6	
Answer	Yes
Document Name	
Comment	
In our opinion, the changes are fraught with problems. First of all, in the NERC definition of System Operator, facilities DO NOT monitor or control the BES, people do. The language as written says otherwise. Second, the inclusion of “and” means a control center must have facilities and people. As automation becomes more prevalent, the definition as written would allow a “control center” that governed thousands (or tens of thousands) of MW of load and/or generation to escape classification as a NERC **Control Center** if it was completely automated, i.e. hosted no people. (Or even today, the “control center” could be personnel free but operators remotely accessed it.) We feel that when considering cyber security, this hardly seems like a change that supports BES reliability. Finally, if the control center definition is going to be amended, it should be modified to fix the ambiguity regarding Transmission facilities. “Two or more locations” while meaningful and clear when describing substations we believe this makes little to no sense on its face when thinking about lines. If the intent is two or more circuits, then the language should plainly say so.	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
See question 1	
Likes 0	
Dislikes 0	
Response	
Thomas Breene - WEC Energy Group, Inc. - 3,4,5,6	
Answer	Yes
Document Name	
Comment	
See question 1.	
Likes 0	
Dislikes 0	

Response	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
See question 1.	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Francis - Midcontinent ISO, Inc. - 2,3 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Poston - Santee Cooper - 1,3,5,6, Group Name Santee Cooper	
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	
Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6	
Answer	
Document Name	
Comment	
Tacoma Power supports the comments of APPA.	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Please see Texas RE’s comments for #1.	

Likes 0	
Dislikes 0	
Response	
Brandon McCormick - Florida Municipal Power Agency - 3,4,5 - FRCC, Group Name FMPA	
Answer	
Document Name	
Comment	
As a CIP standard, most of the commenting will be done by non-operations personnel. It is a concern that the operational impact will not be identified during the balloting and commenting process. This may cause unintentional consequences if the definition is approved.	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	
Document Name	
Comment	
No comment.	
Likes 0	
Dislikes 0	
Response	
George Brown - Acciona Energy North America - 5	
Answer	
Document Name	
Comment	
From a Generator Operator perspective the proposed definition of Control Center does not. The Control Center definition should only define a physical location where Real-time Bulk Electrical System (BES) reliability related operating tasks are performed. It also can include, but cautiously, information on personnel that a Control Center houses, however it should not attempt to define these personnel, either System Operators or operating personnel.	

Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	
Document Name	
Comment	
The California ISO supports the comments of the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	

3. Control Center definition: The SDT contends that there will be no change in BES Cyber System categorization by clarifying the definition of Control Center. This assertion is based on SDT review of the CIP-002-5.1a criteria and its understanding of BES Cyber System categorization through experience implementing CIP-002-5.1a. Do you agree with this assertion? If not, please provide rationale and practical examples of where a change in categorization will occur as a result of this modification.

Brandon McCormick - Florida Municipal Power Agency - 3,4,5 - FRCC, Group Name FMPA

Answer	No
Document Name	

Comment

This new definition may bring in new assets or change the impact level of existing assets which would change the list of BES Cyber Systems and impact levels

Likes 0	
Dislikes 0	

Response

Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body

Answer	No
Document Name	

Comment

SCL supports the APPA submitted comments.

Likes 0	
Dislikes 0	

Response

Marty Hostler - Northern California Power Agency - 5,6

Answer	No
Document Name	

Comment

NCPA does not agree with the SDT assertion that there will be no change in BES Cyber System categorization due to the Control Center definition. This new definition may bring in new assets or change the impact level of existing assets which would change the list of BES Cyber Systems and impact levels.

Likes 0	

Dislikes 0	

Response

Russell Noble - Cowlitz County PUD - 3,5	
Answer	No
Document Name	

Comment
The District supports APPA comment. The current definition draft may pull the District's low impact dispatch center in as a Control Center if further clarifications are not provided. This is due to possible RE identification of the District's ability to independently control for public safety as a "Real-time reliability-related TOP task." Of note, the District's covering Transmission Operator's intent is to remove all TOP Reliable Operation obligation from the District; this assures improved Reliable Operation of the BES by removing a "bucket line" approach to BES critical operations.

Likes 0	
Dislikes 0	

Response

David Francis - Midcontinent ISO, Inc. - 2,3 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG	
Answer	No
Document Name	

Comment
The SRC & ITC SWG also encourages the drafting team to make the requirement forward-looking in regards to contracts currently in place. Provisions should be set for legacy contracts including grandfathering of existing agreements and equipment. Implementation of controls involving telecommunications providers will require coordination and scheduling to align to the providers' resource availability and reduce adverse impact on reliability. This should not require renewal and renegotiation of existing contracts until they reach the end of the existing contract period. It should be noted that it is difficult to determine suitability of the implementation timeline when there are open questions about the viability of available solutions for adequate protections. More time is necessary to allow for coordination with a large number of parties. This will require budgeting, planning, and scheduling with external resources for implementation. It will also require significant testing and validation by parties on both ends of a connection. The SRC & ITC SWG recommends a phased implementation with defined milestones similar to CIP-014. Consider the following: For creation of the plan, 12 months should be allowed to (1) conduct an impact assessments, (2) identify the approach to be included in the plan, (3) implementation milestones, and (4) implementation schedule. This could identify the communication links that have protections currently in place. The

plan could also include identifying all links and protections requiring changes to address service contracts and related relationships to adjust for new protections. The plan could then be approved by an appropriate entity.

For implementation of the plan, additional time should be allowed for budgeting, planning, and scheduling with external resources. This includes planning with other Responsible Entities as well as telecommunications providers.

Likes 0	
Dislikes 0	

Response

Brian Evans-Mongeon - Utility Services, Inc. - 4

Answer	No
Document Name	

Comment

This new definition may bring in new assets or change the impact level of existing assets which would change the list of BES Cyber Systems and impact levels

Likes 0	
Dislikes 0	

Response

David Jendras - Ameren - Ameren Services - 1,3,6

Answer	No
Document Name	

Comment

As noted above, and summarized here, the current enforcement is wide ranging and would incorporate for instance a TOP “control center” that had a meaningful potential impact on the BES without regard to the presence or absence of personnel. While the current Standard may not directly mention this, the wide ranging practical enforcement has included a review of any such facilities. However, we believe that the new definition will absolutely provide an opportunity to avoid compliance obligations by ensuring that no personnel are present at the facility relying instead on automation or remote access.

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Con-Edison and Dominion	
Answer	No
Document Name	
Comment	
This new definition may bring in new assets or change the impact level of existing assets which would change the list of BES Cyber Systems and impact levels.	
Likes 0	
Dislikes 0	
Response	
Lona Calderon - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
This new definition may bring in new assets or change the impact level of existing assets which would change the list of BES Cyber Systems and impact levels	
Likes 0	
Dislikes 0	
Response	
Brandon Cain - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE, Group Name Southern Company	
Answer	No
Document Name	
Comment	
Southern disagrees with the above assertion. Given the assumption that the term "operating personnel" in the current definition is a point of ambiguity and the focus of these Control Center definition changes, Southern has evaluated potential scenarios where a Facility under the current definition would be considered a Control Center, but under the proposed definition, due to ambiguity and interpretation, might not be considered a Control Center, which could ultimately impact your CIP-002-5.1 impact identification and categorization of BES Cyber Systems. The strategy of attempting to remove from scope those lower impact Facilities as Control Centers appears to have the potential to scope out larger impact Facilities as well. We applaud the SDTs efforts in this regard, but recognize that additional discussion and consideration is needed to come up with a better approach to modifying the Control Center definition.	
Likes 0	

Dislikes 0	
Response	
Jack Cashin - American Public Power Association - 4	
Answer	No
Document Name	
Comment	
APPA does not agree with the SDT assertion that there will be no change in BES Cyber System categorization due to the Control Center definition. This new definition may bring in new assets or change the impact level of existing assets which would change the list of BES Cyber Systems and impact levels. If the clarifications APPA (and others) request in question 1 are sufficient, then potentially little or no change in BES Cyber System categorization will occur. However, without adequate clarification, public power believes that there will be significant change in BES Cyber System categorization, should local control rooms become considered as Control Centers.	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
Some entities, registered as Transmission Owners, contract out their Transmission Operator responsibilities but have dispatch centers that are capable of performing tasks on their BES system for safety or maintenance reasons. The current Control Center definition would not automatically classify these dispatch centers as Control Centers. The proposed definition, without clarification, would allow interpretations that may identify these dispatch centers as a Control Center.	
Likes 0	
Dislikes 0	
Response	
Mark Riley - Associated Electric Cooperative, Inc. - 1,3,5,6, Group Name AECI & Member G&Ts	
Answer	No
Document Name	

Comment
The revised Control Center definition may bring in new assets that would be identified by the revised definition. Furthermore, assets such as local control centers/dispatch centers that were not previously considered Control Centers could now be identified as medium impact BES Cyber Systems due to the "functional obligations" language that is present in CIP-002-5.1a Attachment 1, Criterion 2.12.

Likes 0	
Dislikes 0	

Response

Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6	
Answer	No
Document Name	

Comment
Tacoma Power supports the comments of APPA.

Likes 0	
Dislikes 0	

Response

Annette Johnston - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3	
Answer	No
Document Name	

Comment
One of the fundamental purposes for changing the Control Center definition was so Transmission Owners under certain circumstances could have the responsibilities of a Control Therefore, Responsible Entities who previously did not have a Transmission Control Center could have one with this change in definition. There could be other scenarios too, including generation.

Likes 0	
Dislikes 0	

Response

George Brown - Acciona Energy North America - 5	
Answer	Yes
Document Name	

Comment	
From a Generator Operator perspective the proposed definition of Control Center does not.	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
TVA believes adoption of the proposed definition provides useful clarification regarding identification of Low Control Centers.	
Likes 0	
Dislikes 0	
Response	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
ERCOT ISO supports the comments of the ITC SWG.	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
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	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1,3,5,6	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Poston - Santee Cooper - 1,3,5,6, Group Name Santee Cooper	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Amy Folz - Southern Indiana Gas and Electric Co. - 1,3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Austin - AEP - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thomas Breene - WEC Energy Group, Inc. - 3,4,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Shelby Wade - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Theresa Rakowsky - Puget Sound Energy, Inc. - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Greene - SERC Reliability Corporation - 10, Group Name SERC CIPC	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sheranee Nedd - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	
Likes 3	PSEG - PSEG Fossil LLC, 5, Kucey Tim; PSEG - Public Service Electric and Gas Co., 1, Smith Joseph; PSEG - Public Service Electric and Gas Co., 3, Mueller Jeffrey
Dislikes 0	
Response	
Harold Sherrill - Sempra - San Diego Gas and Electric - 7 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Robert Blackney - Edison International - Southern California Edison Company - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	Yes
Document Name	
Comment	
Likes 1	Stephanie Burns, N/A, Burns Stephanie
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Normande Bouffard - Hydro-Qu?bec Production - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Robertson - BC Hydro and Power Authority - 1,3,5, Group Name BC Hydro	
Answer	Yes
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	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response
Richard Vine - California ISO - 2
Answer	
Document Name	
Comment
The California ISO supports the comments of the Security Working Group (SWG)
Likes 0	
Dislikes 0	
Response
Matthew Beilfuss - WEC Energy Group, Inc. - 3,4,5,6 - MRO,RF
Answer	
Document Name	
Comment
No comment
Likes 0	
Dislikes 0	
Response
Rachel Coyne - Texas Reliability Entity, Inc. - 10
Answer	
Document Name	
Comment
Texas RE does not have comments on this question.
Likes 0	
Dislikes 0	
Response

4. Control Center definition: Do you agree with the potential definition of Control Center? If not, please provide rationale or propose an alternative definition.

Annette Johnston - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3

Answer	No
Document Name	

Comment

As expressed in the comments on question 1, the revised Control Center definition doesn't adequately address renewable energy sites. Also, the change in wording to add "capability" potentially broadens the scope.

Likes 0	
Dislikes 0	

Response

Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6

Answer	No
Document Name	

Comment

Tacoma Power supports the comments of APPA.

Likes 0	
Dislikes 0	

Response

Mark Riley - Associated Electric Cooperative, Inc. - 1,3,5,6, Group Name AECI & Member G&Ts

Answer	No
Document Name	

Comment

AECI supports NRECA's comments.

Additionally, the phrase "reliability-related tasks" is not defined and may be misinterpereted by Responsible Entities or compliance enforcement staff. AECI suggests that the SDT clarify the the meaning of this phrase or propose a definition for inclusion in the Glossary of Terms Used in NERC Reliability Standards.

Likes 0	

Dislikes 0	

Response

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	

Comment
Additional clarity is needed with the phrase “operating personnel who perform Real-time reliability-related tasks of…”. If the operating personnel have the capability of performing the real-time reliability-related tasks of a TOP but do not have the authority, it is unclear if their facility would be a Control Center. It is also unclear if the SDT’s goal is to make these facilities Control Centers or not. BPA believes that updating the Control Center definition for CIP standard purposes can potentially cause issues with O&P compliance. BPA recommends broadening scope of the control center definition to include more active engagement from O&P SME’s. More analysis will need to be done once the definition is clarified.

Likes 0	
Dislikes 0	

Response

Jack Cashin - American Public Power Association - 4	
Answer	No
Document Name	

Comment
APPA does not agree with the proposed definition of Control Center based on the need for language clarity in several places. The response to question 1 above provides several examples of where the draft language needs to be changed. Public power believes there are additional language changes that need to be made to the draft definition. The proposed definition uses the NERC defined term “System Operator.” In the NERC Glossary, the “System Operator” definition uses the term “Control Center.” APPA believes this circular dependency of terms needs to be addressed. APPA also requests the SDT clarify the term, “who can act independently to operate or direct the operation.” It is not clear if the operation or direction of this person is specifically addressing that person’s capability or authority to direct or operate. Public power believes this should be clarified. The phrase “Real-time reliability-related tasks” used in the draft definition is not a NERC defined term. APPA believes that the term could be confusing to some NERC compliance personnel who may think it has some relation to the NERC Functional Model. Consequently, public power believes this phrase needs clarification.

Likes 0	
Dislikes 0	

Response

Brandon Cain - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE, Group Name Southern Company

Answer	No
Document Name	

Comment

As noted in #1, above, Southern respectfully disagrees with the approach chosen by the SDT to redefine the term Control Center. The reliability impact of the facility(ies) controlled by the center are an important element of this definition and this aspect did not receive due consideration in the proposed version of the definition.

Likes 0	
Dislikes 0	

Response

Lona Calderon - Salt River Project - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

SRP does not agree with the inclusion of “Transmission Owner” in the following statement, “For Generator Operators, the operating personnel above consist of dispatch personnel at a centrally located dispatch center who receive direction from the Generator Operator’s Reliability Coordinator, Balancing Authority, Transmission Operator, or Transmission Owner, and have the capability to develop specific dispatch instructions for plant operators under their control." By definition, Transmission Owners have no responsibility for operation.

SRP believes the majority of the proposed language in paragraphs 2 through 4 is already expressed within the first paragraph and is redundant. SRP proposes the following language: “One or more facilities, including their associated data centers, that monitor and control the Bulk Electric System (BES) and host operating personnel who perform Real-time reliability-related tasks of any of the following, regardless of NERC registration: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for Transmission Facilities at two or more locations, or 4) a Generator Operator for generation Facilities at two or more locations. These personnel do not include individuals who only execute or relay dispatch instructions without making any modifications.”

The language within the proposed definition of “Control Center” seeks to further identify and define a “System Operator.” This term is already a defined term within the NERC Glossary of terms. Seeking to create a second definition of the term creates confusion and redundancy.

Additionally, SRP agrees with APPA’s comment and requests clarification of what is meant by “Real-time reliability-related tasks.”

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Con-Edison and Dominion	
Answer	No
Document Name	
Comment	
Need clarification(s) – see Q1.	
Likes 0	
Dislikes 0	
Response	
Normande Bouffard - Hydro-Qu?bec Production - 1,5	
Answer	No
Document Name	
Comment	
Alternative proposition for GOP: For Generator Operators, the operating personnel above consist of dispatch personnel at a centrally located dispatch center who receive direction from the Generator Operator's Reliability Coordinator, Balancing Authority, Transmission Operator, or Transmission Owner. These operating personnel only include personnel who can act independently to operate or direct the operation of the Generator Owner's Bulk Electric System Facilities in Real-time.	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 1,3,6	
Answer	No
Document Name	
Comment	
It provides a new gap in enforcement and does not improve the current one where needed.	
Likes 0	
Dislikes 0	
Response	

Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4	
Answer	No
Document Name	
Comment	

FirstEnergy recognizes that the proposed Control Center language describing Transmission Owner operating personnel is to a large degree already used in NERC Reliability Standard PER-005-2 — Operations Personnel Training. However, from a cyber system point of view, it might be beneficial to clarify that these personnel are not inclusive of operating personnel who "can act", which could be interpreted as "who are capable of". There may be personnel who are capable within a location based on cyber system privileges, but who are not authorized, trained, etc. to independently take actions using a cyber system (e.g. IT System Administrators). FirstEnergy recommends the following change to the definition:

For Transmission Owners performing the Real-time reliability-related tasks of a Transmission Operator, the operating personnel above consist of personnel, excluding field switching personnel, who independently operate or direct the operation of the Transmission Owner's Bulk Electric System Transmission Facilities in Real-time

Likes 0	
Dislikes 0	
Response	

Barry Lawson - National Rural Electric Cooperative Association - 3,4	
Answer	No
Document Name	
Comment	

See NRECA's answer to Question 1.

Likes 0	
Dislikes 0	
Response	

Wendy Center - U.S. Bureau of Reclamation - 1,5	
Answer	No
Document Name	
Comment	

Reclamation recommends the first paragraph of the proposed definition revise to state:

One or more agency-designated (i.e., primary or backup) Facilities that host System Operators

Reclamation also recommends that the Control Center definition be restricted to Facilities with the capability to control two or more Facilities that, when combined, are considered high or medium impact rated Facilities.

Reclamation also recommends the SDT consider the implications of whether the Facility has the capability to perform “Real-time reliability-related tasks” with or without hosting System Operators or dispatch personnel.

Likes 0	
Dislikes 0	

Response

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group

Answer	No
Document Name	

Comment

The SPP Standards Review Group has a concern that the term Real-time in the proposed definition does not properly align with the term mention or defined in other Reliability Standards.

Likes 1	Stephanie Burns, N/A, Burns Stephanie
Dislikes 0	

Response

Robert Blackney - Edison International - Southern California Edison Company - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

The proposed definition of Control Center, as written, does not specify whether manned or unmanned data centers are considered facilities associated with a Control Center. NERC should modify the proposed definition to clarify that both manned and unmanned data centers are facilities associated with a Control Center. Specific modifications to the proposed Control Center definition are provided below (modifications are in bold):

“One or more facilities, including their associated **manned or unmanned** data centers, that monitor and control the Bulk Electric System (BES)…”

Likes 0	
Dislikes 0	

Response

Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance

Answer	No
Document Name	

Comment
Note that while Transmission Owners are mentioned in the third paragraph, they are not mentioned in the 4 applicable functions. For completeness, Transmission Owners should be listed as a 5th applicable function. Recommend adding a fifth identification for Transmission Owner for Transmission Facilities who can act independently to operate or direct the operation of the Transmission Owner's Bulk Electric System Transmission Facilities in Real-time to the 1st paragraph definition.

Likes 0	
Dislikes 0	

Response

Brian Evans-Mongeon - Utility Services, Inc. - 4

Answer	No
Document Name	

Comment
See comments to question 1. This definition of uses the NERC defined term "System Operator". In the NERC Glossary, the "System Operator" definition uses the term "Control Center." Request this dependency be addressed. Request clarification of "who can act independently to operate or direct the operation." Is this addressing capability or authority? The phrase "Real-time reliability-related tasks" is not defined and may be determined by some entities or auditors to be associated with the Functional Model. Suggest clarification on the meaning of this phrase

Likes 0	
Dislikes 0	

Response

Sheranee Nedd - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	No
Document Name	
Comment	

The definition is not consistent with PER-005-2 part 4.1.5.1. It uses the statement "*have the capability to* develop specific dispatch instructions… ", where PER-005-2 part 4.1.5.1. states "*may* develop specific dispatch instructions…". There is significant difference between having the capability to do something, versus doing it. The language (i.e."may" versus "having the capability to") concerning Generation and Control Centers (a "centrally located dispatch center" in PER-005-2 part 4.1.5.1) has already been settled by industry, through development and approval of PER-005-2. The proposed definition should stay consistent with PER-005-2 part 4.1.5.1.

Likes 3	PSEG - PSEG Fossil LLC, 5, Kucey Tim; PSEG - Public Service Electric and Gas Co., 1, Smith Joseph; PSEG - Public Service Electric and Gas Co., 3, Mueller Jeffrey
Dislikes 0	
Response	

David Greene - SERC Reliability Corporation - 10, Group Name SERC CIPC	
Answer	No
Document Name	
Comment	

- **Revised Definition:** Second paragraph, change to read "…the operating personnel above *includes* System Operators."

Rationale: Not all operating personnel are technically System Operators

- **Revised Definition:** Third paragraph, change to read "…who *has the ability to act* independently to operate or direct the operation of the Transmission Owner's Bulk Electric System Transmission Facilities in Real-time."

Rationale: To provide clarity that the intent is to include operators that have the ability to act independently even though they might not have the authorization to do so.

Likes 0	
Dislikes 0	
Response	

David Francis - Midcontinent ISO, Inc. - 2,3 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG	
Answer	No
Document Name	
Comment	

In addition to the comments provided in response to question 3, the SRC & SWG offers these comments regarding cost effectiveness. Open Source options to satisfy the requirement to protect communication links and sensitive bulk electric system data communicated between bulk electric systems Control Centers are limited. Few options generally translated to high vendor leverage, which could lead to high implementation costs. It is unclear how or whether costs could be shared among participants in the network. Architectural changes to support these requirements should be spread out over several years. Plus there will be business impacts.

Likes 0	
Dislikes 0	

Response

Shelby Wade - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company

Answer	No
Document Name	

Comment

We support SERC's comments.

Likes 0	
Dislikes 0	

Response

Thomas Breene - WEC Energy Group, Inc. - 3,4,5,6

Answer	No
Document Name	

Comment

See question 1.

Likes 0	
Dislikes 0	

Response

Russell Noble - Cowlitz County PUD - 3,5

Answer	No
Document Name	

Comment
The District supports APPA comment. The District proposes the SDT to consider control rooms restricted to TOP authorized planned maintenance and/or public safety emergency operations as outside the scope of the Control Center definition. If the TO control room is necessary for BES Reliable Operation, then it must be treated as a Control Center. Further, if the covering TOP is able to perform its registered functional obligation without utilizing the TO's control room capabilities, it is counterproductive to add secondary process, i.e., directing the TO personnel, in executing actions to maintain BES within Reliable Operation parameters. The District suggests the following to clarify the intent of identifying a TO control room as a Control Center: One or more facilities, including their associated data centers, that monitor and control the Bulk Electric System (BES) and host operating personnel who perform Real-time reliability-related tasks of: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator, or Transmission Owner performing BES Reliable Operation tasks on behalf of the Transmission Operator, for Transmission Facilities at two or more locations, or 4) a Generator Operator for generation Facilities at two or more locations. For Reliability Coordinators, Balancing Authorities, and Transmission Operators, the operating personnel above appropriately maintain NERC System Operator Certification credentials. For Transmission Owners performing tasks necessary for Bulk Electric System Reliable Operation on behalf of the Transmission Operator, the operating personnel above consist of personnel, excluding field switching personnel lacking Real-time monitoring capability, who can monitor and control the Transmission Owner's Bulk Electric System Transmission Facilities in Real-time as directed by the Transmission Operator's certified operating personnel. Transmission Owner operations related to Transmission Operator authorized planned facility maintenance, and autonomous emergency operations to protect public safety are excluded from this definition.

Likes 0	
Dislikes 0	

Response

Amy Folz - Southern Indiana Gas and Electric Co. - 1,3,5,6 - RF	
Answer	No
Document Name	

Comment
While Vectren understands the need to clarify the Control Center definition and the use of NERC Standard PER-005-2 language to provide clarity, we believe that the language "have the capability to develop" is ambiguous. At Vectren, the operating personnel at the centrally located dispatch center may have the capability to perform, but do not actually perform Real-time Reliability related tasks. PER-005-2 language doesn't mention capability, but rather states that "dispatch personnel at a centrally located dispatch center… may develop dispatch instructions…" We propose that the SDT modify the definition to better align with PER-005-2 language by removing the words "have the capability".

Likes 0	
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion	
Answer	No
Document Name	
Comment	
Please refer the comments in Q1,	
Likes 0	
Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	No
Document Name	
Comment	
AZPS is concerned that, although the SDT intends to align the definition with PER-005-2, the language in the definition leaves ambiguity regarding the genesis of reliability-related tasks. To better ensure this alignment, alleviate the potential for confusion, and enhance clarity, AZPS reiterates its comments provided in response to Question 1 above.	
Likes 0	
Dislikes 0	
Response	
Marty Hostler - Northern California Power Agency - 5,6	
Answer	No
Document Name	
Comment	

1. NCPA does not agree with the proposed definition of Control Center based on the need for language clarity in several places. The response to question 1 above provides several examples of where the draft language needs to be changed.

2. NCPA believes there are other language changes that need to be made to the draft definition. The proposed definition uses the NERC defined term “System Operator.” In the NERC Glossary, the “System Operator” definition uses the term “Control Center.” APPA believes this circular dependency of terms needs to be addressed.

3. NCPA requests the SDT clarify the term, “who can act independently to operate or direct the operation.” It is not clear if the operation or direction of this person is specifically addressing that person’s capability or authority to direct or operate.

Likes 0	
Dislikes 0	

Response

Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body

Answer	No
Document Name	

Comment

SCL supports the APPA submitted comments.

Likes 0	
Dislikes 0	

Response

Brandon McCormick - Florida Municipal Power Agency - 3,4,5 - FRCC, Group Name FMPA

Answer	No
Document Name	

Comment

This definition of uses the NERC defined term “System Operator”. In the NERC Glossary, the “System Operator” definition uses the term “Control Center.” Request this dependency be addressed.

Request clarification of “who can act independently to operate or direct the operation.” Is this addressing capability or authority?

The phrase “Real-time reliability-related tasks” is not defined and may be determined by some entities or auditors to be associated with the Functional Model. Suggest clarification on the meaning of this phrase

Likes 0	
Dislikes 0	

Response

George Brown - Acciona Energy North America - 5

Answer	No
Document Name	

Comment

The Control Center definition should only define a physical location where Real-time Bulk Electrical System (BES) reliability related operating tasks are performed. It also can include, but cautiously, information on personnel that a Control Center houses, however it should not attempt to define these personnel, either System Operators or operating personnel.

If it is the intention of the SDT to define operating personnel of a Transmission Owner (TO) performing the Real-time reliability-related operating tasks of a Transmission Operator and Generator Operator (GOP) operating personnel, then a separate term needs to be defined to identify these individuals.

Data centers usually do not host personnel and the Control Center definition needs to be modified to account for this.

In the context of the proposed definition of Control Center, in the Generator Operator section, the term “direction” is used, “Operating Instruction” is already a defined term and should be used instead of “direction”. Also, the term “capability” is used and is inaccurate, many individuals have the capability to modify a generator, i.e. IT/OT personnel, however, few have the authority; “capability should be modified to “authority”.

The following is suggested:

Control Center: One or more facilities that monitor and control the Bulk Electric System and host System Operators and Operating Personnel who perform the Real-time operating reliability related-tasks, and includes the associated data centers, of:

1) a Reliability Coordinator,

2) a Balancing Authority,

3) a Transmission Operator for Transmission Facilities at two or more locations,

4) a Transmission Owner performing the delegated Real-time reliability-related operating tasks of a Transmission Operator at two or more locations or

5) a Generator Operator for generation Facilities at two or more locations.

Operating Personnel: An individual at a Control Center of a Transmission Owner or Generator Operator who perform the Real-time operating reliability related-tasks as follows:

1. For a Transmission Owner these individuals would be personnel who can act independently and have the authority to operate or direct the operation of the Transmission Owner’s Bulk Electric System Transmission Facilities in Real-time.

2. For a Generator Operator these individuals would be personnel who receive Operating Instructions from the Generator Operator’s Reliability Coordinator, Balancing Authority, Transmission Operator, or Transmission Owner, and have the authority to develop and direct specific dispatch instructions for plant operators under their control. These personnel do not include plant operators located at a generator plant site or personnel at a centrally located dispatch center who relay Operating Instructions and dispatch instructions without making any modifications.

Likes 0	
Dislikes 0	

Response

Matthew Beilfuss - WEC Energy Group, Inc. - 3,4,5,6 - MRO,RF	
Answer	No
Document Name	
Comment	

Adjusting the NERC defined term for Control Center to facilitate the expansion of CIP-002 scope to additional cyber assets is not appropriate. In particular, the inclusion of Transmission Owner and lengthy definition of operating personnel does not belong in the NERC Glossary of Terms. If a CIP project team identifies a class of cyber assets that can impact the BES (a gap in the existing standards), approaches that expand the definition of a Control Center beyond what is understood by industry potentially limits use of the term in other standards.

Below is a proposed revision, please note we have included the operating personnel of a TO for illustrative purposes, we do not believe it belongs in the Control Center definition.

One or more facilities, including their associated data centers that monitor and control the Bulk Electric System (BES) and host System Operators, or any of the following;

- ***operating personnel of a Generator Operator that have the ability to develop specific dispatch instructions for plant operators under their control at two or more locations***
- ***operating personnel of a Transmission Owner who can act independently to operate or direct the operation of the Transmission Owner's Bulk Electric System Transmission Facilities in Real-time.***

Likes 0	
Dislikes 0	

Response

Jamie Monette - Allete - Minnesota Power, Inc. - 1

Answer	Yes
Document Name	

Comment

With modification in question 1.

Likes 0	
Dislikes 0	

Response

Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2

Answer	Yes
Document Name	

Comment

ERCOT ISO supports the comments of the ITC SWG.

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 agrees with the proposed changes to the definition of Control Center, but would like to recommend the drafting team consider the following revision to the first sentence in the first paragraph of the definition:

One or more facilities, including their associated data centers, that host operating personnel who monitor and control the Bulk Electric system (BES) by performing Real-time reliability-related tasks of: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for Transmission Facilities at two or more locations, or 4) a Generator Operator for generation Facilities at two or more locations.

For Reliability Coordinators, Balancing Authorities, and Transmission Operators, the operating personnel above are System Operators.

For Transmission Owners performing the Real-time reliability-related tasks of a Transmission Operator, the operating personnel above consist of personnel, excluding field switching personnel, who can act independently to operate or direct the operation of the Transmission Owner's Bulk Electric System Transmission Facilities in Real-time.

For Generator Operators, the operating personnel above consist of dispatch personnel at a centrally located dispatch center who receive direction from the Generator Operator's Reliability Coordinator, Balancing Authority, Transmission Operator, or Transmission Owner, and have the capability to develop specific dispatch instructions for plant operators under their control. These personnel do not include plant operators located at a generator plant site or personnel at a centrally located dispatch center who relay dispatch instructions without making any modifications.

As currently written, the first sentence of the first paragraph of the proposed definition, it seems to imply that it is the Facilities that monitor and control the BES, however, it should actually read that the operating personnel are responsible for monitoring and controlling of the BES. We feel that the above is a more accurate statement, and better reflects the current state of operations.

Likes 0	
Dislikes 0	

Response

Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	
Response	
Patricia Robertson - BC Hydro and Power Authority - 1,3,5, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Harold Sherrill - Sempra - San Diego Gas and Electric - 7 - WECC	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Theresa Rakowsky - Puget Sound Energy, Inc. - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Austin - AEP - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
James Poston - Santee Cooper - 1,3,5,6, Group Name Santee Cooper	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
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	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Please see Texas RE's comments to #1.	
Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	
Document Name	
Comment	
The California ISO supports the comments of the Security Working Group (SWG)	

Likes 0	
Dislikes 0	
Response	

5. Implementation Plan: The SDT proposes to make the new Control Center definition effective upon applicable governmental authority's order approving the definition, or as otherwise provided for by the applicable governmental authority. Do you agree with this proposal not to provide additional implementation time following approval? If you agree with the potential implementation time period, please note the actions you will take that require this amount of time to complete. If you think an alternate implementation time period is needed, please propose an alternate implementation period and provide a detailed explanation of actions and time needed to meet your proposed implementation deadline.

George Brown - Acciona Energy North America - 5

Answer	No
Document Name	

Comment

From a Generator Operator perspective the proposed definition of Control Center should not affect current operations. However, the proposed definition of Control Center applies to a new Functional Entity, the Transmission Owner, and as such an implementation plan/period will be required. Transmission Owner's should suggest an appropriate plan/period.

Likes 0	
Dislikes 0	

Response

Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body

Answer	No
Document Name	

Comment

SCL supports the APPA submitted comments.

Likes 0	
Dislikes 0	

Response

Amy Folz - Southern Indiana Gas and Electric Co. - 1,3,5,6 - RF

Answer	No
Document Name	

Comment

Vectren respectfully requests the SDT consider that Responsible Entities which are impacted by these changes should have at least 12 months to implement the new definition, similar to other NERC operational and CIP standards.

Likes 0	
Dislikes 0	

Response

Shelby Wade - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company

Answer	No
Document Name	

Comment

We support SERC's comments.

Likes 0	
Dislikes 0	

Response

David Greene - SERC Reliability Corporation - 10, Group Name SERC CIPC

Answer	No
Document Name	

Comment

- **Alternate Implementation Period:** *2 Year* Implementation Plan Period

Rationale: There are a number of factors to consider, and all affect the time required to implement, to include the following:

-
    - Complexity of the technology solutions to be implemented,
    - Number of interconnecting lines to secure,
    - Troubleshooting/testing at each connection point, and
    - Coordination requirements with external stakeholders

Likes 0	
Dislikes 0	

Response

Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance

Answer	No
Document Name	

Comment

Would recommend at least a 30 day implementation period upon applicable governmental authority approval to allow entities appropriate time to make any necessary changes to policies, procedures and other necessary administrative documentation and make notification and training as necessary.

Likes 0	
Dislikes 0	

Response

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group

Answer	No
Document Name	

Comment

The SPP Standards Review Group has developed an interpretation based on discussions from the CIP SDT, it's believed that this is just a definition change and no additional implementation time. If this does involve an additional implementation time, we believe 18 months is better than 12 months. Due to technological changes needed to secure the data and collaboration between sending and receiving party, we feel more time is needed to implement the standard.

Likes 1	Stephanie Burns, N/A, Burns Stephanie
Dislikes 0	

Response

Wendy Center - U.S. Bureau of Reclamation - 1,5

Answer	No
Document Name	

Comment

Eighteen calendar months after the approval of the control center definition and the CIP-012-1 standard to allow entities time to evaluate the impact of the changes effected by the new standard and implement an appropriate response.

Likes 0	

Dislikes 0	
Response	
Barry Lawson - National Rural Electric Cooperative Association - 3,4	
Answer	No
Document Name	
Comment	
NRECA requests that the Implementation Plan (IP) be revised to provide a 24 month period of time for registered entities that do not meet the current Control Center definition, but under a revised Control Center definition they do have a Control Center. This 24 month time period is necessary to provide registered entities enough time to deal with procurement and budget cycles, and the implementation of the required technical and procedural controls for a “low, medium or high” category Control Center.	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	No
Document Name	
Comment	
Idaho Power proposes that additional implementation time be provided to evaluate the effect of the new definition and to ensure applicable protections/controls are in place. Idaho Power believes 6 to 12 months would be appropriate.	
Likes 0	
Dislikes 0	
Response	
Normande Bouffard - Hydro-Qu?bec Production - 1,5	
Answer	No
Document Name	
Comment	
12 to 18 months needed for new control center	
Likes 0	

Dislikes 0	
Response	
Lona Calderon - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
SRP agrees with APPA and LPPC that this commenting should not be included along with comments to CIP standards. By doing so, the personnel working exclusively with 693 standards are being excluded and may cause unintentional consequences.	
Likes 0	
Dislikes 0	
Response	
Mark Riley - Associated Electric Cooperative, Inc. - 1,3,5,6, Group Name AECI & Member G&Ts	
Answer	No
Document Name	
Comment	
AECI supports NRECA's response to Question 5.	
Likes 0	
Dislikes 0	
Response	
Annette Johnston - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3	
Answer	No
Document Name	
Comment	
The Implementation Plan for other standards provide that unplanned changes could result in a low impact categorization where previously the asset containing BES Cyber Systems had no categorization. Categorization changes due to this definition should be treated that same... Under these circumstances for CIP version 5, Responsible Entities were to comply with all Requirements applicable to low impact BES Cyber Systems within 12 months following the identification and categorization of the affected BES Cyber System.	
Likes 0	

Dislikes 0	
Response	
Aaron Austin - AEP - 3,5	
Answer	Yes
Document Name	
Comment	
AEP suggests that the SDT include explicit reference to the section of Implementation Plan for Version 5 CIP Cyber Security Standards for unplanned changes.	
Likes 0	
Dislikes 0	
Response	
Russell Noble - Cowlitz County PUD - 3,5	
Answer	Yes
Document Name	
Comment	
The District believes the proposed timing for the implementation plan is appropriate. The Implementation Plans for in the existing CIP Standards will cover newly identified Control Centers.	
Likes 0	
Dislikes 0	
Response	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
ERCOT ISO supports the comments of the ITC SWG.	
Likes 0	

Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
With regards to CIP, this wouldn't be a problem. I cannot speak for others that would be impacted.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Con-Edison and Dominion	
Answer	Yes
Document Name	
Comment	
Yes, because the Implementation Plan in the CIP Standards will cover newly identified assets.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE	
Answer	Yes
Document Name	
Comment	
The company will review current systems and protections against the approved Control Center glossary term and as part of CIP-012-1 implementation.	
Likes 0	
Dislikes 0	

Response
Jack Cashin - American Public Power Association - 4
Answer	Yes
Document Name	
Comment
APPA believes the proposed timing for the implementation plan is appropriate. The Implementation Plans for in the existing CIP Standards will cover newly identified Control Centers.
Likes 0	
Dislikes 0	
Response
Nicholas Lauriat - Network and Security Technologies - 1
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
Leonard Kula - Independent Electricity System Operator - 2

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Poston - Santee Cooper - 1,3,5,6, Group Name Santee Cooper	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Marty Hostler - Northern California Power Agency - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Theresa Rakowsky - Puget Sound Energy, Inc. - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sheranee Nedd - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	
Likes 3	PSEG - PSEG Fossil LLC, 5, Kucey Tim; PSEG - Public Service Electric and Gas Co., 1, Smith Joseph; PSEG - Public Service Electric and Gas Co., 3, Mueller Jeffrey

Dislikes 0	
Response	
Harold Sherrill - Sempra - San Diego Gas and Electric - 7 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Robert Blackney - Edison International - Southern California Edison Company - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 1,3,6	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Robertson - BC Hydro and Power Authority - 1,3,5, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brandon Cain - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	
Document Name	
Comment	
The California ISO supports the comments of the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	
Matthew Beilfuss - WEC Energy Group, Inc. - 3,4,5,6 - MRO,RF	
Answer	
Document Name	
Comment	
No comment	
Likes 0	
Dislikes 0	
Response	
Brandon McCormick - Florida Municipal Power Agency - 3,4,5 - FRCC, Group Name FMPA	
Answer	
Document Name	
Comment	
This seems appropriate for CIP because the Implementation Plans in the other CIP Standards will cover newly identified Control Centers. It is unclear of the impact on Operations so it also unclear on the implementation of any changes to operations	
Likes 0	
Dislikes 0	
Response	

Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Absent a specific implementation plan, Texas RE understands the definition would be effective upon FERC approval.	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	
Document Name	
Comment	
This seems appropriate for CIP because the Implementation Plans in the other CIP Standards will cover newly identified Control Centers. It is unclear of the impact on Operations so it also unclear on the implementation of any changes to operations.	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	
Document Name	
Comment	
BPA believes that the implementation period is dependent on the clarification of what will or what should become a control center.	
Likes 0	
Dislikes 0	
Response	

Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6	
Answer	
Document Name	
Comment	
Tacoma Power supports the comments of APPA.	
Likes 0	
Dislikes 0	
Response	

6. If you have additional comments on the proposed definition of Control Center that you have not provided in response to the questions above, please provide them here.

Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6

Answer	
Document Name	

Comment

Tacoma Power supports the comments of APPA.

Likes 0	
Dislikes 0	

Response

Jack Cashin - American Public Power Association - 4

Answer	
Document Name	

Comment

APPA thanks the SDT for the opportunity to comment.

Likes 0	
Dislikes 0	

Response

Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE

Answer	
Document Name	

Comment

None.

Likes 0	
Dislikes 0	

Response

Lona Calderon - Salt River Project - 1,3,5,6 - WECC	
Answer	
Document Name	
Comment	
SRP is concerned the SDT presented this proposed definition under CIP only. This could result in missing comments from a broader 693 audience who will be affected by this definition change.	
Likes 0	
Dislikes 0	
Response	
Barry Lawson - National Rural Electric Cooperative Association - 3,4	
Answer	
Document Name	
Comment	
NRECA appreciates the continued efforts of the CIP SDT.	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 1,5	
Answer	
Document Name	
Comment	
None.	
Likes 0	
Dislikes 0	
Response	
Harold Sherrill - Sempra - San Diego Gas and Electric - 7 - WECC	
Answer	

Document Name	

Comment

· SDG&E desires clarification on the definition of “associated data centers”. Is it the data centers that house the Industrial Controls Systems (ICS) or is it all data centers that support the “control center”?

· The language in the proposed definition excludes oral communication, but could email be considered “data used for Operational Planning Analysis, Real-time Assessments, and Real-time monitoring”?

· The proposed definition states: “One or more facilities, including their associated data center, that monitor and control the BES……” SDG&E recommends the following change: “One or more facilities, including their associated data center, used to monitor and control the BES……”

-In sections where “Transmission Operator” is mentioned the term *BES* should be inserted before “Transmission Facilities…”

- In sections where “Generator Operator” is mentioned the term *BES* should be inserted before Generator Operator for “Generation Facilities….”

· SDG&E believes clarity could be given to the words: “have the capability to develop specific dispatch instructions for plant operators under their control.”

- SDG&E seeks clarification on the phrase: “centrally located dispatch center who relay dispatch instructions without making any modifications.”

Likes 0	
Dislikes 0	

Response

Sheranee Nedd - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs

Answer	
Document Name	

Comment

It is unclear if/how RC “backup control center” facilities or TOP/BA “backup functionality” required for RC and TOPs/BAs, respectively, by NERC reliability standard EOP-008, are addressed by the proposed definition.

Likes 3	PSEG - PSEG Fossil LLC, 5, Kucey Tim; PSEG - Public Service Electric and Gas Co., 1, Smith Joseph; PSEG - Public Service Electric and Gas Co., 3, Mueller Jeffrey
Dislikes 0	

Response

Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	
Document Name	
Comment	

CenterPoint Energy Houston Electric, LLC believes the revisions to the Control Center definition more accurately identify Control Centers.

Likes 0	
Dislikes 0	
Response	

David Francis - Midcontinent ISO, Inc. - 2,3 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG

Answer	
Document Name	
Comment	

The SRC & ITC SWG asserts that the proposed standard does not make clear how entities should work together when addressing security concerns across a communication network link. If both entities work with CIP Standard assumptions on both ends of a communication network, some support for joint handling of issues could be made clear. However, if only one entity is CIP-compliant for a given link, the current standard draft does not make clear the extent of protection expected for the data. The Standard should provide more information on the ownership of obligations for protecting the entire link

It is unclear whether the addition of CIP-012 affects the exemptions of communication networks in any of the applicability sections of other standards (CIP-002 through CIP-011). The SWG requests clarification that CIP-012 fills in some of the gap created the CIP-002 – CIP-011 third party telecommunications exemption (4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.)

It has been ten years since the SANDIA report ("Secure ICCP Considerations and Recommendations"), the only detailed report on this subject which could be considered close having entered mainstream awareness in the industry. Today, as ten years ago, Secure ICCP is not a viable choice for utilities, if only due to limited community experience and vendor support, not to mention the complexities of key management. The transition strategies that SANDIA discusses – Layer 3 protection using IPsec and Layer 2 protection with hardware encryption – remain today's target solutions.

IPsec is a viable alternative. Over MPLS, IPsec could secure GRE tunnels between CE routers. Challenges with this approach include the possibility of having to hire a third party to manage certificates and IPsec links, especially for ISOs that do not manage their own MPLS networks.

The SRC & ITC SWG position on security architecture is that business transactions (such as ICCP) should not be tightly coupled with encryption technologies. Solutions should prefer network overlays versus security extensions to a protocol (such as Secure ICCP or DNP3 SA).

The security architecture should prefer least-latent encryption solutions at the Ethernet or IP layers of the network stack. MACsec (802.1AE) models the spirit of an optimal solution within a metro area – could it scale wider?

The SRC & ITC SWG's overall position on Secure ICCP is that it represents too much reliability risk. The ITC SWG is concerned about the lack of open standards and protocols available to meet the confidentiality and integrity security objectives of CIP-012. Assuming that a solution involves encryption, the only two open standards and protocols that can meet the CIP-012 security objectives are IPsec and TLS. The potential for vendor leverage in such a small open solution space is large. Vendor-managed MPLS networks, typical among utilities, already entrench high annual telecommunication costs in utility budgets. Security vendors continue to benefit from the expense of establishing layered cyber defenses. Open Source solutions provide a cost and agility refuge from this lopsided value chain without compromising defense layers. The trend toward managed services makes the cost problem worse for utilities, especially in the context of insufficiently evaluated risk. Vendor leverage only grows given the practical consideration that all the communicating parties in a WAN of connected real-time Control Centers would need to adopt a common solution in order to minimize complexity and cost.

Likes 0	
Dislikes 0	

Response

Theresa Rakowsky - Puget Sound Energy, Inc. - 1,3,5

Answer	
Document Name	

Comment

n/a

Likes 0	
Dislikes 0	

Response

Thomas Breene - WEC Energy Group, Inc. - 3,4,5,6

Answer	
Document Name	

Comment

N/A

Likes 0	
Dislikes 0	

Response

Russell Noble - Cowlitz County PUD - 3,5	
Answer	
Document Name	
Comment	
Thank you for the opportunity to comment.	
Likes 0	
Dislikes 0	
Response	
Aaron Austin - AEP - 3,5	
Answer	
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	
Amy Folz - Southern Indiana Gas and Electric Co. - 1,3,5,6 - RF	
Answer	
Document Name	
Comment	
Vectren is committed to the safety and reliability of the BES and committed to compliance excellence. We appreciate the efforts of the Standard Drafting Team and will be glad to provide any additional detail upon request. Thank you for allowing Vectren the opportunity to provide comments on this draft definition.	
Likes 0	
Dislikes 0	
Response	

Marty Hostler - Northern California Power Agency - 5,6	
Answer	
Document Name	
Comment	
No additional comments.	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1,3,5,6	
Answer	
Document Name	
Comment	
No comments	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	
Document Name	
Comment	
SCL supports the APPA submitted comments. Our primary concern here is that it is not appropriate to ballot in CIP only for a far-reaching change that can impact both O&P and CIP standards.	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	

Document Name	
Comment	
Texas RE does not have additional comments.	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	
Document Name	
Comment	
TVA agrees with the proposed definition of Control Center.	
Likes 0	
Dislikes 0	
Response	
George Brown - Acciona Energy North America - 5	
Answer	
Document Name	
Comment	
No further comments.	
Likes 0	
Dislikes 0	
Response	
Matthew Beilfuss - WEC Energy Group, Inc. - 3,4,5,6 - MRO,RF	
Answer	
Document Name	
Comment	

No ocmment	
Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	
Document Name	
Comment	
The California ISO supports the comments of the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	

Comment Report

Project Name:	2016-02 Modifications to CIP Standards | Technical Rationale and Justification for CIP-012-1
Comment Period Start Date:	8/14/2017
Comment Period End Date:	9/12/2017
Associated Ballots:	

There were 42 sets of responses, including comments from approximately 137 different people from approximately 92 companies representing 10 of the Industry Segments as shown in the table on the following pages.

Questions

1. The SDT developed draft Technical Rationale and Justification for CIP-012-1 to provide stakeholders and the ERO Enterprise an understanding of the technology and technical requirements in the Reliability Standard. Do you agree that the draft Technical Rationale and Justification for CIP-012-1 clearly explains the technical reasoning for the proposed standard? If you do not agree, or if you agree but have comments or suggestions for the draft document, please provide your recommendation and explanation.

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim	1,3,4	RF	FirstEnergy Corporation	Aaron Ghdooshim	FirstEnergy - FirstEnergy Corporation	4	RF
					Aubrey Short	FirstEnergy - FirstEnergy Corporation	1	RF
					Theresa Ciancio	FirstEnergy - FirstEnergy Corporation	3	RF
					Robert Loy	FirstEnergy - FirstEnergy Solutions	5	RF
					Ann Ivanc	FirstEnergy - FirstEnergy Solutions	6	RF
Southern Company - Southern Company Services, Inc.	Brandon Cain	1,3,5,6	FRCC,MRO,NPCC,SERC,SPP RE,Texas RE,WECC	Southern Company	Katherine Prewitt	Southern Company - Southern Company Services, Inc.	1	SERC
					R. Scott Moore	Southern Company - Alabama Power Company	3	SERC
					William D. Shultz	Southern Company - Southern Company Generation	5	SERC
					Jennifer Sykes	Southern Company - Southern Company Generation and Energy Marketing	6	SERC
Florida Municipal Power Agency	Brandon McCormick	3,4,5	FRCC	FMPA	Tim Beyrle	City of New Smyrna Beach Utilities Commission	4	FRCC
					Jim Howard	Lakeland Electric	5	FRCC

					Lynne Mila	City of Clewiston	4	FRCC
					Javier Cisneros	Fort Pierce Utilities Authority	3	FRCC
					Randy Hahn	Ocala Utility Services	3	FRCC
					Don Cuevas	Beaches Energy Services	1	FRCC
					Jeffrey Partington	Keys Energy Services	4	FRCC
					Tom Reedy	Florida Municipal Power Pool	6	FRCC
					Steven Lancaster	Beaches Energy Services	3	FRCC
					Mike Blough	Kissimmee Utility Authority	5	FRCC
					Chris Adkins	City of Leesburg	3	FRCC
					Ginny Beigel	City of Vero Beach	3	FRCC
Midcontinent ISO, Inc.	David Francis	2,3	FRCC,MRO,NPCC,RF,SERC,SPP RE,Texas RE,WECC	SRC + SWG	Gregory Campoli	New York Independent System Operator	2	NPCC
					Mark Holman	PJM Interconnection, L.L.C.	2	RF
					Charles Yeung	Southwest Power Pool, Inc. (RTO)	2	SPP RE
					Terry BIlke	Midcontinent ISO, Inc.	2	RF
					Elizabeth Axson	Electric Reliability Council of Texas, Inc.	2,3	Texas RE
					Ben Li	IESO	1	MRO
					Drew Bonser	SWG	NA - Not Applicable	NA - Not Applicable
					Darrem Lamb	CAISO	2	WECC

					Matt Goldberg	ISONE	2	NPCC
SERC Reliability Corporation	David Greene	10	SERC	SERC CIPC	Bill Peterson	SERC RRO	10	SERC
					Mike Hagee	SERC RRO	10	SERC
					SERC CIPC	Various	1,2,5,9	SERC
Con Ed - Consolidated Edison Co. of New York	Dermot Smyth	1,3,5,6	NPCC	Con Edison	Dermot Smyth	Con Edison Company of New York	1,3,5,6	NPCC
					Edward Bedder	Orange & Rockland		NPCC
Seattle City Light	Ginette Lacasse	1,3,4,5,6	WECC	Seattle City Light Ballot Body	Pawel Krupa	Seattle City Light	1	WECC
					Hao Li	Seattle City Light	4	WECC
					Bud (Charles) Freeman	Seattle City Light	6	WECC
					Mike Haynes	Seattle City Light	5	WECC
					Michael Watkins	Seattle City Light	1,4	WECC
					Faz Kasraie	Seattle City Light	5	WECC
					John Clark	Seattle City Light	6	WECC
					Tuan Tran	Seattle City Light	3	WECC
					Laurrie Hammack	Seattle City Light	3	WECC
Santee Cooper	James Poston	1,3,5,6		Santee Cooper	Rene' Free	Santee Cooper	1	SERC
					Rodger Blakely	Santee Cooper	1	SERC
					Chris Jimenez	Santee Cooper	1	SERC
					Troy Lee	Santee Cooper	1	SERC
					Tom Abrams	Santee Cooper	1	SERC
					Jennifer Richards	Santee Cooper	1	SERC
					Stony Martin	Santee Cooper	1	SERC
					Glenn Stephens	Santee Cooper	1	SERC
					Tom Perry	Santee Cooper	1	SERC
	Patricia Robertson	1,3,5		BC Hydro	Patricia Robertson	BC Hydro and Power Authority	1	WECC

BC Hydro and Power Authority					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	1,2,3,4,5,6,7,8,9,10	NPCC	RSC no Con-Edison and Dominion	Guy V. Zito	Northeast Power Coordinating Council	10	NPCC
					Randy MacDonald	New Brunswick Power	2	NPCC
					Wayne Sipperly	New York Power Authority	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	Orange & Rockland Utilities	3	NPCC
					Michele Tondalo	UI	1	NPCC
					Laura Mcleod	NB Power	1	NPCC
					Michael Schiavone	National Grid	1	NPCC
					Michael Jones	National Grid	3	NPCC
					David Ramkalawan	Ontario Power Generation Inc.	5	NPCC
					Quintin Lee	Eversource Energy	1	NPCC
					Kathleen Goodman	ISO-NE	2	NPCC
					Greg Campoli	NYISO	2	NPCC
					Silvia Mitchell	NextEra Energy - Florida Power and Light Co.	6	NPCC

					Paul Malozewski	Hydro One Networks, Inc.	3	NPCC
					Sylvain Clermont	Hydro Quebec	1	NPCC
					Helen Lainis	IESO	2	NPCC
					Chantal Mazza	Hydro Quebec	2	NPCC
Southwest Power Pool, Inc. (RTO)	Shannon Mickens	2	SPP RE	SPP Standards Review Group	Shannon Mickens	Southwest Power Pool Inc.	2	SPP RE
					Deborah McEndaffer	Midwest Energy, Inc.	NA - Not Applicable	SPP RE
					Don Schmit	Nebraska Public Power District	5	SPP RE
					Louis Guidry	Cleco Corporation	1,3,5,6	SPP RE
					Robert Hirchak	Cleco Corporation	6	SPP RE
					Marty Paulk	Cleco Corporation	1,3,5,6	SPP RE
					Michelle Corley	Cleco Corporation	3	SPP RE
					Robert Gray	Board of Public Utilities	NA - Not Applicable	SPP RE
					Ron Spicer	EDP Renewables	NA - Not Applicable	SPP RE
					Steven Keller	Southwest Power Pool	2	SPP RE
					Laura Cox	Westar Energy	5	SPP RE
PPL - Louisville Gas and Electric Co.	Shelby Wade	3,5,6	RF,SERC	Louisville Gas and Electric Company and Kentucky Utilities Company	Charles Freibert	PPL - Louisville Gas and Electric Co.	3	SERC
					Dan Wilson	PPL - Louisville Gas and Electric Co.	5	SERC
					Linn Oelker	PPL - Louisville Gas and Electric Co.	6	SERC
PSEG	Sheranee Nedd	1,3,5,6	NPCC,RF	PSEG REs	Tim Kucey	PSEG - PSEG Fossil LLC	5	RF
					Karla Jara	PSEG Energy Resources and Trade LLC	6	RF

					Jeffrey Mueller	PSEG - Public Service Electric and Gas Co	3	RF
					Joseph Smith	PSEG - Public Service Electric and Gas Co	1	RF

1. The SDT developed draft Technical Rationale and Justification for CIP-012-1 to provide stakeholders and the ERO Enterprise an understanding of the technology and technical requirements in the Reliability Standard. Do you agree that the draft Technical Rationale and Justification for CIP-012-1 clearly explains the technical reasoning for the proposed standard? If you do not agree, or if you agree but have comments or suggestions for the draft document, please provide your recommendation and explanation.

Leonard Kula - Independent Electricity System Operator - 2

Answer	No
Document Name	

Comment

The IESO offers the following comments:

- On page 5, under the Control Center Ownership section, the following statement is confusing, “Applying protection among a Responsible Entity’s owned Control Centers is solely at its discretion.” Our understanding is that choosing to apply protections is not at our discretion, it is required. We recommend the following, “The method of applying protection to Control Center’s exclusively owned by a Responsible Entity is solely at its discretion. However, when multiple Responsible Entities own a Control Center at either end of the communication link, applying protection requires additional coordination and diligence.”
- Recommend that the rationale state that the standard does not increase the scope of BES Cyber Systems that require protections under CIP-002 thru CIP-011. The requirements apply only to the protection of the data that is transmitted across infrastructure not owned by a Responsible Entity.
- Implementation guidance is needed on the use of armored cable as a physical security protection method when using leased or subscribed fiber with multiple telecom carriers in the path. The guidance needs to address router hops and fiber patch panels that exist within a telecom provider’s central office.

Likes 0	
Dislikes 0	

Response

Dermot Smyth - Con Ed - Consolidated Edison Co. of New York - 1,3,5,6, Group Name Con Edison

Answer	No
Document Name	

Comment

Please disregard answer above. This was an error. I am unable to change it. We have no comments on this item. Dermot Smyth.

Likes 0	
Dislikes 0	

Response

David Rivera - New York Power Authority - 1,3,5,6	
Answer	No
Document Name	
Comment	
While the CIP standards should emphasize outcomes and allow entities to achieve specific security objectives in many ways, protections applied to communications should be evaluated with due consideration of the context in which people, processes and technology are applied to establish a given security protection. Demonstration of risk mitigation should include assessment of not just technology and process to provide protection, but also the diversity and severity of threats present in a given context (e.g. the difference between dedicated communication links as opposed to broadly shared communications infrastructure). Particular technology and process applied in a context with fewer or lower likelihood threats should be preferred over the same technology and process in a context with more or greater likelihood threats (i.e. greater overall risk). Simply specifying that some (how much?) risk mitigation should be applied by means that include physical, logical and possibly other means leads to insufficient conditions for establishing compliance both for the responsible entity and anyone reviewing compliance for that entity. Entities should consider not only that risk mitigation should take place, but also the thresholds for residual risk that should be considered acceptable for such communication.	
Likes 0	
Dislikes 0	
Response	
Brandon McCormick - Florida Municipal Power Agency - 3,4,5 - FRCC, Group Name FMPA	
Answer	No
Document Name	
Comment	
FMPA does not agree that the Technical Rationale and Justification for CIP-012-1 fully explains the technical reasoning for the standard. The Rationale document does not provide justification for the Operational Planning and Analysis data that is included in the scope of this standard. While the document does provide an example of communication paths (page 5), the example would be improved by adding a communication path between the TOP Control Center and the GOP Control Center.	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	No
Document Name	

Comment
SCL supports APPA comments

Likes 0	
Dislikes 0	

Response

Marty Hostler - Northern California Power Agency - 5,6	
Answer	No
Document Name	

Comment
This document does not provide justification for the inclusion of the Operational Planning and Analysis data. NCPA suggests it be removed from the standards scope.

Likes 0	
Dislikes 0	

Response

Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	No
Document Name	

Comment
AZPS provides the following comments for the SDT's consideration: 1. The statement provided in "General Considerations for Requirement R1" clearly limits the applicability of Requirement R1 to the real-time horizon and does not indicate Requirement R1 being applicable to the Operational Planning Horizon. Specifically, the technical justification states that the focus is on "developing a plan to protect information that is critical to the real-time operations of the Bulk Electric System." This is in direct conflict with the draft standard, which scopes the plan to "to mitigate the risk of the unauthorized disclosure or modification of data used for Operational Planning Analysis, Real-time Assessment, and Real-time monitoring data." AZPS reiterates its comments in response to the draft CIP-012-1 that the inclusion of data used for Operational Planning Analysis does not have a meaningful impact on reliability or real-time operations for the BES such that extending protection to Operational Planning Analysis results in overall benefits to reliability. 2. AZPS is concerned that the rationale provided in "Alignment with IRO and TOP standards" may misalign with the IRO Standards. The IRO and TOP Standards explicitly allow each responsible entity to develop individual data specifications because responsible entity processes can differ based upon operational characteristics, coordinated functional registrations, delegation agreements, operating agreements, etc. Statements within that section that these requirements force consistency in data and data specifications appear to directly conflict with the intent and flexibility of the IRO and TOP data specification requirements. 3. AZPS also suggests revising the third sentence in the section entitled "Control Center Ownership" because that sentence, read alone, absolves a responsible entity from protecting communications between its own control centers. The sentence in question reads "Applying protection

among a Responsible Entity's owned Control Centers is solely at its discretion." This sentence also seems to conflict with the first sentence in the same section.	
Likes 0	
Dislikes 0	
Response	
Aaron Austin - AEP - 3,5	
Answer	No
Document Name	
Comment	
The document makes a good case for the security needed for Real-time data. It does not treat the Planning and Analysis data as well. Please see the AEP comments in the Unofficial Comment Form for CIP-012-1.	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	No
Document Name	Project 2016-02_CIP-012-1_NSRF Final.docx
Comment	
WAPA feels there is additional need for clarity and proposed language as identified in the NSRF comments.	
Likes 0	
Dislikes 0	
Response	
Russell Noble - Cowlitz County PUD - 3,5	
Answer	No
Document Name	
Comment	
Cowlitz PUD supports comment submitted by APPA.	

Likes 0	
Dislikes 0	

Response

David Francis - Midcontinent ISO, Inc. - 2,3 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG

Answer	No
Document Name	

Comment

The SRC & ITC SWG offers the following comments:

On page 5, under the Control Center Ownership section, the following statement is confusing, “Applying protection among a Responsible Entity’s owned Control Centers is solely at its discretion.” Our understanding is that choosing to apply protections is not at our discretion, it is required. We recommend the following, “The method of applying protection to Control Center’s exclusively owned by a Responsible Entity is solely at its discretion. However, when multiple Responsible Entities own a Control Center at either end of the communication link, applying protection requires additional coordination and diligence.”

Recommend that the rationale state that the standard does not increase the scope of BES Cyber Systems that require protections under CIP-002 thru CIP-011. The requirements apply only to the protection of the data that is transmitted across infrastructure not owned by a Responsible Entity.

Implementation guidance is needed on the use of armored cable as a physical security protection method when using leased or subscribed fiber with multiple telecom carriers in the path. The guidance needs to address router hops and fiber patch panels that exist within a telecom provider’s central office.

Likes 0	
Dislikes 0	

Response

Michael Puscas - ISO New England, Inc. - 2

Answer	No
Document Name	

Comment

In order to evaluate the extent and kind of obligation involved, the definition of between control centers needs to be clearer with regard to the communication link. What are the demarcation points for obligation to show compliance? Should there be explicit agreements with each end of the communication link to arrange such demarcation? How should responsible entities deal with third parties involved with trust relationships in communication links (i.e. telecommunications providers managing routers)?

Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	No
Document Name	
Comment	

A) It is understood that the reference model shown on page 5 is an example of communication paths. Suggest adding the communication path between the TOP Control Center and the GOP Control Center to provide further clarity.

B) This document does not provide justification for the inclusion of the Operational Planning and Analysis data is included in the scope of this standard. Suggest that this be added to the Technical Rationale and Justification document or this data be removed from the scope of the standard.

Likes 0	
Dislikes 0	
Response	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	

ERCOT ISO supports the comments of the ITC SWG.

The ITC SWG offers the following comments:

- On page 5, under the Control Center Ownership section, the following statement is confusing, “Applying protection among a Responsible Entity’s owned Control Centers is solely at its discretion.” Our understanding is that choosing to apply protections is not at our discretion, it is required. We recommend the following, “The method of applying protection to Control Center’s exclusively owned by a Responsible Entity is solely at its discretion. However, when multiple Responsible Entities own a Control Center at either end of the communication link, applying protection requires additional coordination and diligence.”

- Recommend that the rationale state that the standard does not increase the scope of BES Cyber Systems that require protections under CIP-002 thru CIP-011. The requirements apply only to the protection of the data that is transmitted across infrastructure not owned by a Responsible Entity.

- Implementation guidance is needed on the use of armored cable as a physical security protection method when using leased or subscribed fiber with multiple telecom carriers in the path. The guidance needs to address router hops and fiber patch panels that exist within a telecom provider's central office.

Likes 0	
Dislikes 0	

Response

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group

Answer	No
Document Name	

Comment

The SPP Standards Review Group recommends that the drafting team includes other Standards that are identified in question #2 comment form (Glossary of Terms Used in NERC Reliability Standards-Control Center). From our perspective, the technical documents only mention the applicable TOP and IRO Standards. If other standards are identified that are potentially impacted by this definition change, they need to be included in that the documentation to help support justification as well as showing consistency.

Likes 1	Stephanie Burns, N/A, Burns Stephanie
Dislikes 0	

Response

James Gower - Entergy - NA - Not Applicable - SERC

Answer	No
Document Name	

Comment

The standard as drafted explicitly excludes oral communications, but does not consider forms of written communication (email, chat, etc) that could communicate the same type of information that an oral communication could. These written instructions are commonly outside of SCADA systems and are on corporate systems, and this standard would require physical or logical controls on those systems for communications that may traverse these systems. The standard should specify the protection of "operational data", "BCS Data", or some other term to clarify protection of data outside of instructions, or provide data validation (i.e verify emails by phone) as an acceptable control.

Additionally, Entergy has concerns over expanding the scope of protection from "real-time" as defined in other CIP standards and through existing CIP definitions, to require the protection of Operational Planning Analysis data that is outside of the "real-time" horizon.

Likes 0	
Dislikes 0	

Response

Wendy Center - U.S. Bureau of Reclamation - 1,5

Answer	No
Document Name	

Comment

Reclamation recommends the NIST definitions of “confidentiality” and “integrity” be added to the NERC Glossary of Terms Used in Reliability Standards, rather than referring to NIST Special Publication 800-53A, Revision 4.

Reclamation also recommends the Drafting Team state clearly that examples provided in Technical Rationale and Justification documents are neither mandatory, nor enforceable, nor the only method of achieving compliance.

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Con-Edison and Dominion

Answer	No
Document Name	

Comment

While the CIP standards should emphasize outcomes, and allow entities to achieve specific security objectives in many ways, protections applied to communications should be evaluated with due consideration of the context in which people, processes and technology are applied to establish a given security protection. Demonstration of risk mitigation should include assessment of not just technology and process to provide protection, but also the diversity and severity of threats present in a given context (e.g. the difference between dedicated communication links as opposed to broadly shared communications infrastructure). Particular technology and process applied in a context with fewer or lower likelihood threats should be preferred over the same technology and process in a context with more or greater likelihood threats (i.e. greater overall risk). Simply specifying that some (how much?) risk mitigation should be applied by means that include physical, logical and possibly other means leads to insufficient conditions for establishing compliance both for the responsible entity and anyone reviewing compliance for that entity. Entities should consider not only that risk mitigation should take place, but also the thresholds for residual risk that should be considered acceptable for such communication.

Likes 0	
Dislikes 0	

Response

Lona Calderon - Salt River Project - 1,3,5,6 - WECC

Answer	No

Document Name	

Comment

This document does not address what equally effective methods are or what appropriate physical controls may be. It also does not discuss where physical controls may or may not be appropriate over logical controls such as encryption. SRP also does not believe the document addresses latency or computer resource concerns. SRP requests additional guidance on what would be acceptable for these items.

SRP also agrees with APPA's recommendation to provide justification for the inclusion of the Operational Planning and Analysis data in the scope of this standard.

Likes 0	
Dislikes 0	

Response

Brandon Cain - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE, Group Name Southern Company

Answer	No
Document Name	

Comment

Southern disagrees with the Technical Rationale and Justification for CIP-012 for several reasons. We feel that the "data centric approach" being pursued opens the door for misinterpretation and the unintentional scoping-in of data that does not require protection. We are concerned that under the proposed Standard, the efforts required in redefining the data to be protected will obscure the true intent of the standard which is to protect the communications links over which the data travels. We feel that clarification of the scope of the data to be protected is essential for ensuring that the correct communications links are secured and the standard can be properly implemented via an appropriate technical solution. As currently written, Southern feels that the scope is too broad and the protections required would be cost prohibitive.

Likes 0	
Dislikes 0	

Response

Jack Cashin - American Public Power Association - 4

Answer	No
Document Name	

Comment

APPA does not agree that the Technical Rationale and Justification for CIP-012-1 fully explains the technical reasoning for the standard. The document does not address what equally effective methods are, or what appropriate physical controls may be. Nor does it discuss where physical controls may or may not be appropriate over logical controls such as encryption. In addition, latency and computer resource concerns are not addressed.

The Rationale document does not provide justification for the Operational Planning and Analysis data that is included in the scope of this standard.

While the document does provide an example of communication paths (page 5), the example would be improved by adding a communication path between the TOP Control Center and the GOP Control Center.

Likes 0	
Dislikes 0	

Response

Annette Johnston - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3

Answer	No
Document Name	

Comment

MidAmerican Energy Company comments on the CIP-012 focused on two major areas which impact the Technical Rationale and Justification document.

One,we do not agree with two separate requirements, one for a plan and one to implement. We recommend following precedent in the other CIP standards, for example, CIP-004 through CIP-011. The obligation can be accomplished with one requirement,

Two, the scoping for sensitive data should be explicitly to information exchanged between Control Centers' BES Cyber Systems. This corresponds to SDT's assertation that "this data resides within BES Cyber Systems, and while at rest is protected by CIP-003 through CIP-011." It also corresponds to FERC's recognition in their order that certain entities are already required to exchange necessary real-time and operational planning data through secured networks using mutually agreeable security protocol.

Additionally, the Technical Rationale and Justification document creates a higher bar than the obligation in the requirement and should be changed. Specifically, expectation levels are different between the requirement “to mitigate the risk of the unauthorized disclosure or modification of data” and Technical Rationale and Justification's second sentence in the General Consideration for R2 section on page six, which states, “The protection must prevent unauthorized disclosure or modification of applicable data”. “Must prevent” is a higher bar than “mitigate the risk of.” The sentence on page 6 should be changed to match the sentence in the requirement.

MidAmerican Energy Company's comments on the proposed Control Center definition reflect concerns that renewable generation resources such as wind and solar are insufficiently addressed. While the concept of alignment with PER-005-2 has merit, PER-005-2 is antiquated in the reference to "plant operators located at a generator plant site." Renewable resources do not fit the traditional "plant site" or "plant operators" model of historical traditional generating plants. (The diagram on page five represents these as "control rooms." We agree with excluding the plant operators at the plant site for traditional generation. It must also be clear that the operating personnel at wind and solar farms are also excluded.

Corresponding to the comment above, the diagram on page 5 of the Technical Rationale and Justification should include a box to demonstrate with a red dashed line that renewables operating personnel are also out-of-scope for Control Center communications.

Also in the diagram, we are trying to understand the two BA Control Center boxes. Why does one have no field assets depicted?

Also in the diagram, there is a box for "GOP control room." Shouldn't this be labeled as a GO control room?

Likes 0	
Dislikes 0	

Response

Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6

Answer	No
Document Name	

Comment

Tacoma Power supports the comments of APPA.

Likes 0	
Dislikes 0	

Response

Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC

Answer	Yes
Document Name	

Comment

However we are concerned because unauthorized alteration Operational Planning Analysis data does not pose a threat to the BES. This should be addressed by TOP 010-1 regarding the quality of the data. Accordingly, we are not clear on the utility of the standard since TOP 010-1 will mitigate the risk. Operational Planning Data is not real time data.

The SDT should consider exempting Email as they did with oral communication because of its use for communicating Operational Planning Data. We suggest that the SDT communicate the risk related to operational planning analysis data.

We would also like more guidance on key management and inter utility agreements on key management. Whatever measures implemented to meet compliance, it would increase operational burden and decrease reliability.

It may be more cost effective if an industry wide initiative is conducted with encryption specifications. There may be issues with entities using divergent technologies and measures to prevent an uncoordinated mismatched implementation that should be addressed. This initiative requires an industry wide standard, entities cannot decide individually to implement encryption schemes without coordination.

Likes 0	
Dislikes 0	

Response

David Ramkalawan - Ontario Power Generation Inc. - 5

Answer	Yes
Document Name	

Comment

OPG understands the focus is on protection of data communication between control centers but would like to clarify that it is not being required to verify integrity of data from it's origination points to the point where it's first aggregated at a control center, as this would be a substantially more difficult and costly requirement to achieve.

Likes 0	
Dislikes 0	

Response

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	Yes
Document Name	

Comment

While BPA agrees that the draft Technical Rationale and Justification for CIP-012-1 clearly explains the technical reasoning for the proposed standard, BPA does not agree that the intent of FERC Order No. 822 has been met. Order No. 822 requires implementation of controls to protect, at a minimum,

communication links AND sensitive BES data communicated between BES Control Centers. However, the SDT is providing latitude to protect communication links, data or both. BPA recommends placing controls on the data (encryption where availability requirements are not negatively impacted) AND end points (physical controls) where technically feasible.

Additionally, BPA has concerns about the SDT's assumption that "availability" is adequately addressed by other NERC standards (TOP-001-4 and IRO-002-5), as discussed in the "Overview of confidentiality and integrity" section of the Technical Rationale and Justification.

1. The proposed language includes protection of "confidentiality and integrity of data" but excludes "availability" from the language of the requirement. However, in the Confidentiality/Integrity/Availability (CIA) triad for information security, each leg must be balanced against the other two legs. By segregating Availability to TOP-001-4 and IRO-002-5, while leaving Confidentiality/Integrity in the proposed CIP-012 standard, it becomes impossible to properly balance all three legs of the triad to achieve optimum Reliability of the BES. The cyber security triad represents design tradeoffs; entities can't properly design communications networks – or worse: existing infrastructure may need to be rebuilt – if one of the options (Availability) is removed from consideration.

2. While TOP-001-4 and IRO-002-5 (redundancy and diverse routing of data) can be used to increase Availability, Availability can also be achieved through other equally effective methods. Therefore, "Availability" is not adequately addressed by TOP-001-4 and IRO-002-5 and limits entities' options to address availability by other methods more appropriate to their systems.

Therefore, BPA proposes that "availability" be included in the Technical Rationale and Justification to meet the security objectives of Order 822, i.e., "…to protect AVAILABILITY, confidentiality and integrity of data required for reliable operation...."

BPA also encourages the SDT to use the Guidelines and Technical Basis section to recognize the distinction between the engineering/design term "availability" (in which availability is quantitative – e.g., a system is designed to be available 99.99% of the time) and the cyber security application in which availability is a qualitative element of security that is constantly balanced against two other (often competing) elements (confidentiality and integrity).

Likes 0	
Dislikes 0	

Response

Nicholas Lauriat - Network and Security Technologies - 1

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Chris Scanlon - Exelon - 1,3,5,6

Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
James Poston - Santee Cooper - 1,3,5,6, Group Name Santee Cooper	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Shelby Wade - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Theresa Rakowsky - Puget Sound Energy, Inc. - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
David Greene - SERC Reliability Corporation - 10, Group Name SERC CIPC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sheranee Nedd - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	
Likes 3	PSEG - PSEG Fossil LLC, 5, Kucey Tim; PSEG - Public Service Electric and Gas Co., 1, Smith Joseph; PSEG - Public Service Electric and Gas Co., 3, Mueller Jeffrey
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4, Group Name FirstEnergy Corporation	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Robertson - BC Hydro and Power Authority - 1,3,5, Group Name BC Hydro	
Answer	Yes
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	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	
Document Name	
Comment	
The California ISO supports the comments of the Security Working Group (SWG).	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE understands that the intent of a Technical Rationale document, as presented to the NERC Members Representative Committee on August 9, 2017, is to provide stakeholders and the ERO Enterprise an understanding of the technology and technical requirements of the Reliability Standard. However, the majority of this Technical Rationale Document for proposed Reliability Standard CIP-012-1 appear to be Implementation Guidance. Texas RE recommends following the process for submitting Implementation Guidance for the content of this document. Texas RE addressed its concerns with CIP-012-1 in its comments on the requirement language. Please refer to Texas RE's comments on the proposed draft of CIP-012-1. If, in the future, a draft Implementation Guidance is posted for review, Texas RE will evaluate it at that point.	

Likes 0	
Dislikes 0	
Response	
Normande Bouffard - Hydro-Qu?bec Production - 1,5	
Answer	
Document Name	
Comment	
N/A,	
Likes 0	
Dislikes 0	
Response	

Comments from Sean Erickson, WAPA

Questions

1. Requirement R1: The SDT drafted CIP-012-1 Requirement R1 to meet the mandatory requirement for the Responsible Entity to develop one or more documented plan(s) to mitigate the risk of the unauthorized disclosure or modification of data used for Operational Planning Analysis, Real-time Assessment, and Real-time monitoring data while being transmitted between Control Centers. Do you agree with this revision? If not, please provide the basis for your disagreement and an alternate proposal.

   ☐ Yes

   ☒ No

   Comments: As mentioned by the SDT, FERC directs *that "…require responsible entities to implement controls to protect, at a minimum, communication links and sensitive bulk electric system data communicated between bulk electric system Control Centers…"*. First, having a plan does not add to the reliability of protecting said data. This is an unwarranted layer of compliance that is not needed. Everything does not need a plan in order to be protected. Recommend that R1 be written in parallel to the FERC directive, which does not require a plan (per the SDTs Consideration of Issues and Directives).

   If "Plan" is maintained in CIP-012-1 then, the SDT should explain what is meant by having a Plan? Per CIP-003-6 it states, The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan

can describe an approach involving multiple procedures to address a broad subject matter. Is a plan the template document which is used throughout our Standards or is it a set of controls that show that the data is being protected per R1? The NSRF does not understand why a Plan is needed when the data is being protected by physical or electronic means. If a Plan is required, then all the Plan is going to say is that the cabling that transfers data is in a protected conduit (or other means) between Control Centers.

Secondly, The NSRF questions why the SDT is not in line with the FERC Order to "…protect …data…" but the proposed R1 states to "…mitigate the risk of unauthorized discloser or modification of data…"?

R1 should be rewritten to state: "The responsible entity shall have controls (or other understandable words) in place to protect against the unauthorized disclosure or modification of BES data used for Operational Planning Analysis, Real-time Assessments, and Real-time monitoring while being transmitted between BES Control Centers. This excludes oral communications". Please note that the word "BES" is needed within R1 regardless of it our proposed rewrite is accepted or not.

2. Requirement R1: The SDT seeks comment on the need to scope sensitive BES data as it applies to Operational Planning Analysis, Real-time Assessment, and Real-time monitoring. Do you agree with scoping CIP-012-1 Requirement R1 in this manner? Please provide comment in support of your response.

   ☐ Yes

   ☒ No

   Comments: The SDT needs to add "BES" data into the language as recommended above in question 1.

3. Implementation Plan: The SDT revised the Implementation Plan such that the standard and NERC Glossary terms are effective the first day of the first calendar quarter that is twelve (12) calendar months after the effective date of the applicable governmental authority's order approving the standard, or as otherwise provided for by the applicable governmental authority. Do you agree with this proposal? If you agree with the proposed implementation time period, please note the actions you will take that require this amount of time to complete. If you think an alternate implementation time period is needed – shorter or longer - please propose an alternate implementation plan and provide a detailed explanation of actions and time needed to meet the implementation deadline.

   ☐ Yes

   ☒ No

   Comments: The 12 month time period may only work for Entities who are vertically intergraded. The flow of applicable BES data within CIP-012-1 can be viewed as a "spider web" of data transfer for large RC foot-prints. With this being said, there may be non-compliance issues when one side of the data transference is protected and the other side is not. The SDT should propose a phased in approach to protecting data. A five (5) year implementation plan will allow entities to fund these projects. This is especially import to small entities. Per the NERC Guidance concerning "Phase Implementation Plans with Completion Percentages (http://www.nerc.com/pa/comp/guidance/CMEPPracticeGuidesDL/CMEP_Practice_Guide_Phased_Implementation_Completion_Percentages.pdf) please state that the CIP-012-1 does not fall under this guidance.

4. The SDT believes proposed CIP-012-1 provides entities with flexibility to meet the reliability objectives in a cost effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost effective approaches, please provide your recommendation and, if appropriate, technical justification.

☒ Yes

☐ No

Comments: Thank you for adding the third bullet of R1.

5. If you have additional comments on the proposed CIP-012-1 – Cyber Security -- Communication Networks drafted in response to the FERC directive that you have **not** provided in response to the questions above, please provide them here.

Comments:

1. The NSRF questions the use of "Real-time monitoring" as an applicable object within R1. "Real-time" is defined as "present time as opposed to future time". Which our industry understands and without the word "monitoring" being defined, may lead to misinterpretation by responsible entities and CEAs, alike. The word "monitoring" may mean ALL monitoring of an entity's entire SCADA system. It should be the "monitoring" of BES data, only, that is required for Operational Planning Analysis and Real-time Assessments.

2. The Applicability section states, "For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly". This proposed Standard does not specify any specific entities and recommend that this be removed.

3. The NSRF has concerns with the proposed definition of Control Center. The largest issue is the last paragraph concerning a Generating Operator. The use of the word "capability" is ambiguous and will confuse Registered Entities and CEAs, a like. The SDT should consider the approved Applicability within PER-005-2 part 4.1.5.1, which reads:

Dispatch personnel at a centrally located dispatch center who receive direction from the Generator Operator's Reliability Coordinator, Balancing Authority, Transmission Operator, or Transmission Owner, and may develop specific dispatch instructions for plant operators under their control. These personnel do not include plant operators located at a generator plant site or personnel at a centrally located dispatch center who relay dispatch instructions without making any modifications.

This aligns with current and understood wording of PER-005-2.

4. Are the noted "Real-time reliability related- tasks" within the proposed definition, the same "Real-time Reliability-related task prescribed in PER-005-2? If so, please state this in your consideration of comments document and within your guidance document.

5. The NSRF believes that data associated with Operational Planning Analyses (OPA), Real-time monitoring (RTm), and Real-time Assessments (RTA) are predicated on other Standards and protection of data is required but all three areas (OPA, RTm, and RTA) are not subject equally to the Applicable Entities noted in CIP-012-1. Per IRO-010-2, R1, the RC is to document its specifications necessary for OPA, RTm, and RTA. Per TOP-003-3, R1 the TOP is to document its specifications necessary for OPA, RTm, and RTA. Per TOP-003-3, R2, the BA is to document its

specifications necessary for analysis functions and RTm, only. The SDT, in the Technical Rationale and Justification document acknowledges TOP-003 and IRO-010 "provides consistent scoping of identified data" [R1 section: Alignment with IRO and TOP Standards"]. The SDT should quantify that the data to be protected is the data associated with the Applicable entities with IRO-010-2 and TOP-003-3. With doing this, the SDT will articulate what the entity is to preform what analysis and what "data" is to be protected, based on already approved NERC Reliability Standards. By clearly identifying (and linking) the data to be protected from the data specifications developed under Standards TOP-003 and IRO-010, there is no room for interpretation of what "data" is to be protected.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the second draft of the proposed standard.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23 - April 21, 2016
SAR posted for comment	June 1 – June 30, 2016
Informal comment period	February 10- March 13, 2017
45-day formal comment period with additional ballot	July 27 – September 11, 2017
45-day formal comment period with additional ballot	October 27 – December 11, 2017

Anticipated Actions	Date
10-day final ballot	TBD
Board	TBD

A. Introduction

1. **Title:** Cyber Security – Communications between Control Centers

2. **Number:** CIP-012-1

3. **Purpose:** To protect the confidentiality and integrity of Real-time Assessment and Real-time monitoring and control data transmitted between Control Centers.

4. **Applicability:**

   4.1. Functional Entities: The requirements in this standard apply to the following functional entities, referred to as "Responsible Entities," that own or operate a Control Center.

   4.1.1. Balancing Authority

   4.1.2. Generator Operator

   4.1.3. Generator Owner

   4.1.4. Reliability Coordinator

   4.1.5. Transmission Operator

   4.1.6. Transmission Owner

   4.2. **Exemptions:** The following are exempt from Reliability Standard CIP-012-1:

   4.2.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

   4.2.2. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

5. **Effective Date:** See Implementation Plan for CIP-012-1.

B. Requirements and Measures

R1. The Responsible Entity shall develop one or more documented plan(s) to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring and control data while being transmitted between any Control Centers. This requirement excludes oral communications. The plan shall include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. Identification of security protection used to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring and control data while being transmitted between Control Centers;

1.2. Identification of demarcation point(s) where security protection is applied for transmitting Real-time Assessment and Real-time monitoring and control data between Control Centers; and

1.3. Identification of roles and responsibilities of each Responsible Entity for applying security protection to the transmission of Real-time Assessment and Real-time monitoring and control data between Control Centers, when the Control Centers are owned or operated by different Responsible Entities.

M1. Evidence may include, but is not limited to, documented plan(s) that meet the security objective of Requirement R1.

R2. The Responsible Entity shall implement the plan(s) specified in Requirement R1, except under CIP Exceptional Circumstances.

M2. Evidence may include, but is not limited to, documentation demonstrating implementation of the plans developed pursuant to Requirement R1.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" means NERC, the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

- The Responsible Entities shall keep data or evidence of each Requirement in this Reliability Standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The Compliance Enforcement Authority (CEA) shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or

information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	N/A	The Responsible Entity documented its plan(s) but failed to include one of the applicable parts of the plan as specified in Requirement R1.	The Responsible Entity documented its plan(s) but failed to include two of the applicable parts of the plan as specified in Requirement R1.	The Responsible Entity failed to document plan(s) for Requirement R1.
R2.	N/A	N/A	N/A	The Responsible Entity failed to implement its plan(s) as specified in Requirement R1, except under CIP Exceptional Circumstances.

D. Regional Variances

None.

E. Associated Documents

Implementation Plan.

Version History

Version	Date	Action	Change Tracking
1	TBD	Respond to FERC Order No. 822	N/A

Standard Attachments

None.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the ~~first~~second draft of the proposed standard.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23 - April 21, 2016
SAR posted for comment	June 1 – June 30, 2016
Informal comment period	February 10- March 13, 2017
45-day formal comment period with additional ballot	July 27 – September 11, 2017
45-day formal comment period with additional ballot	October 27 – December 11, 2017

Anticipated Actions	Date
~~45-day formal comment period with additional ballot~~	~~TBD~~
10-day final ballot	TBD
Board	TBD

~~Upon Board adoption, the rationale boxes will be moved to the Supplemental Material Section.~~

A. Introduction

1. **Title:** Cyber Security – Communications between Control ~~Center Communication Networks~~ Centers

2. **Number:** CIP-012-1

3. **Purpose:** To protect the confidentiality and integrity of Real-time Assessment and Real-time monitoring and control data transmitted between Control Centers ~~required for reliable operation of the Bulk Electric System (BES).~~.

4. **Applicability:**

   4.1. Functional Entities: ~~For the purpose of the~~The requirements ~~contained herein,~~in this standard apply to the following ~~list of~~ functional entities ~~will be collectively,~~ referred to as "Responsible Entities~~." For requirements in this standard where a specific functional entity,~~" that own or ~~subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.~~operate a Control Center.

   4.1.1. Balancing Authority

   4.1.2. Generator Operator

   4.1.3. Generator Owner

   4.1.4. Reliability Coordinator

   4.1.5. Transmission Operator

   4.1.6. Transmission Owner

   4.2. **Exemptions:** The following are exempt from Reliability Standard CIP-012-1:

   4.2.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

   4.2.2. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

5. **Effective Date:** See Implementation Plan for CIP-012-1.

B. Requirements and Measures

~~**Rationale for Requirements R1 and R2:** FERC Order No. 822 directed NERC to develop modifications to the CIP Reliability Standards to require Responsible Entities to implement controls to protect communication links and sensitive Bulk Electric System (BES) data communicated between BES Control Centers. Reliability Standard CIP-012-1 responds to that directive, requiring Responsible Entities to develop a plan to protect the confidentiality and integrity of sensitive data while being transmitted between Control Centers. Responsible~~

~~Entities use various means to communicate information between Control Centers. The plan for protecting these communications is required for all impact levels due to the inter-dependency of multiple impact levels.~~

~~The type of data in scope of CIP-012-1 is data used for Operational Planning Analyses, Real-time Assessments, and Real-time monitoring. The terms Operational Planning Analyses, Real-time Assessments, and Real-time used are defined in the Glossary of Terms Used in NERC Reliability Standards and used in TOP-003 and IRO-010, among other Reliability Standards.~~

~~There are differences between the plan(s) required to be developed and implemented for CIP-012-1 and the protection required in CIP-006-6 Requirement R1 Part 1.10. CIP-012-1 Requirements R1 and R2 protect the applicable data during transmission between two geographically separate Control Centers. CIP-006 Requirement R1 Part 1.10 protects nonprogrammable communication components within an Electronic Security Perimeter (ESP) but outside of a Physical Security Perimeter (PSP). The transmission of applicable data between Control Centers takes place outside of an ESP. Therefore, the protection contained in CIP-006-6 Requirement R1 Part 1.10 does not apply.~~

R1. The Responsible Entity shall develop one or more documented plan(s) to mitigate the risk of ~~the~~ unauthorized disclosure or modification of ~~data used for Operational Planning Analysis,~~ Real-time ~~Assessments,~~Assessment and Real-time monitoring and control data while being transmitted between any Control Centers. This requirement excludes oral communications. The plan shall include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

~~**1.1.** Risk mitigation shall be accomplished by one or more of the following actions:~~

- ~~Physically protecting the communication links transmitting the data;~~
- ~~Logically protecting the data during transmission; or~~

~~**1.2.**~~**1.1.** ~~Using an equally effective method~~Identification of security protection used to mitigate the risk of unauthorized disclosure or modification of ~~the data.~~ Real-time Assessment and Real-time monitoring and control data while being transmitted between Control Centers;

~~Note: If the Responsible Entity does not have a Control Center or it does not transmit the type of data specified in Requirement R1 of CIP-012-1 between two Control Centers, the requirements in CIP-012-1 would not apply to that entity.~~

1.2. Identification of demarcation point(s) where security protection is applied for transmitting Real-time Assessment and Real-time monitoring and control data between Control Centers; and

1.3. Identification of roles and responsibilities of each Responsible Entity for applying security protection to the transmission of Real-time Assessment and Real-time monitoring and control data between Control Centers, when the Control Centers are owned or operated by different Responsible Entities.

M1. Evidence may include, but is not limited to, documented plan(s) that meet the security objective of Requirement R1.

R2. The Responsible Entity shall implement the plan(s) specified in Requirement R1, except under CIP Exceptional Circumstances.

M2. Evidence may include, but is not limited to, documentation ~~to demonstrate~~demonstrating implementation of ~~methods to mitigate~~ the ~~risk of the unauthorized disclosure or modification of data in~~plans developed pursuant to Requirement R1.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" means NERC ~~or~~, the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The ~~applicable entity~~Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

- The Responsible Entities shall keep data or evidence of each Requirement in this Reliability Standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The Compliance Enforcement Authority (CEA) shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	N/A	~~N/A~~ The Responsible Entity documented its plan(s) but failed to include one of the applicable parts of the plan as specified in Requirement R1.	~~N/A~~The Responsible Entity documented its plan(s) but failed to include two of the applicable parts of the plan as specified in Requirement R1.	The Responsible Entity failed to document ~~one or more~~ plan(s) ~~that achieve the security objective to mitigate the risk of unauthorized disclosure or modification of data used~~ for ~~Operational Planning Analysis, Real-time Assessments, and Real-time monitoring while being transmitted, excluding oral communication, between Control Centers as specified in~~ Requirement R1.
R2.	N/A	N/A	N/A	The Responsible Entity failed to implement its plan(s) ~~to mitigate the risk of unauthorized disclosure or modification of data used for Operational Planning Analysis, Real-time Assessments, and Real-time~~

				~~monitoring while being transmitted, excluding oral communication, between Control Centers~~ as specified in Requirement R1, except under CIP Exceptional Circumstances.

D. Regional Variances

None.

E. Associated Documents

Implementation Plan.

Version History

Version	Date	Action	Change Tracking
1	TBD	Respond to FERC Order No. 822	N/A

Standard Attachments

None.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2016-02 Modifications to CIP Standards
Reliability Standard CIP-012-1

Applicable Standard

- Reliability Standard CIP-012-1 - Cyber Security – Communications between Control Centers

Requested Retirements

- None

Prerequisite Standard

These standard(s) or definitions must be approved before the Applicable Standard becomes effective:

- None

Applicable Entities

- Balancing Authority
- Generator Operator
- Generator Owner
- Reliability Coordinator
- Transmission Operator
- Transmission Owner

Effective Date

Reliability Standard CIP-012-1 - Cyber Security – Communications between Control Centers

Where approval by an applicable governmental authority is required, Reliability Standard CIP-012-1 shall become effective on the first day of the first calendar quarter that is twenty-four (24) calendar months after the effective date of the applicable governmental authority's order approving the standard, or as otherwise provided for by the applicable governmental authority.

Where approval by an applicable governmental authority is not required, Reliability Standard CIP-012-1 shall become effective on the first day of the first calendar quarter that is twenty-four (24) calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2016-02 Modifications to CIP Standards
Reliability Standard CIP-012-1

Applicable Standard

- Reliability Standard CIP-012-1 - Cyber Security – Communications between Control ~~Center Communication Networks~~Centers

Requested Retirements

- None

Prerequisite Standard

These standard(s) or definitions must be approved before the Applicable Standard becomes effective:

- None

Applicable Entities

- Balancing Authority
- Generator Operator
- Generator Owner
- Reliability Coordinator
- Transmission Operator
- Transmission Owner

Effective Date

Reliability Standard CIP-012-1 - Cyber Security – Communications between Control ~~Center Communication Networks~~Centers

Where approval by an applicable governmental authority is required, Reliability Standard CIP-012-1 shall become effective on the first day of the first calendar quarter that is ~~twelve (12~~twenty-four (24) calendar months after the effective date of the applicable governmental authority's order approving the standard, or as otherwise provided for by the applicable governmental authority.

Where approval by an applicable governmental authority is not required, Reliability Standard CIP-012-1 shall become effective on the first day of the first calendar quarter that is ~~twelve (12~~twenty-four (24) calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Comment Form

Project 2016-02 Modifications to CIP Standards
CIP-012-1

Do not use this form for submitting comments. Use the Standards Balloting and Commenting System (SBS) to submit comments on **CIP-012-1 – Cyber Security – Communications between Control Centers.** Comments must be submitted by **8 p.m. Eastern, Monday, December 11, 2017.**

Additional information is available on the project page. If you have questions, contact Katherine Street at (404) 446-9702 or Mat Bunch at (404) 446-9785.

Background Information

On January 21, 2016, the Commission issued Order No. 822, approving seven CIP Reliability Standards and new or modified definitions, and directing modifications to the CIP Reliability Standards. Among others, the Commission directed NERC to "develop modifications to the CIP Reliability Standards to require responsible entities to implement controls to protect, at a minimum, communication links and sensitive bulk electric system data communicated between bulk electric system Control Centers in a manner that is appropriately tailored to address the risks posed to the bulk electric system by the assets being protected (i.e., high, medium, or low impact)." (Order 822, Paragraph 53)

The Project 2016-02 Standard Drafting Team (SDT) drafted Reliability Standard CIP-012-1 to require Responsible Entities to implement controls to protect sensitive Bulk Electric System (BES) data while being transmitted over communications links between BES Control Centers. Due to the sensitivity of the data being communicated between the Control Centers the standard applies to all impact levels (i.e., high, medium, or low impact).

The SDT drafted requirements allowing Responsible Entities to apply protection to the links, the data, or both, to satisfy the security objective consistent with the capabilities of the Responsible Entity's operational environment. Requirement R1 requires Responsible Entities to document one or more plans that protect Real-time Assessment and Real-time monitoring and control data while being transmitted between Control Centers. The plan(s) must address how the Responsible Entity will mitigate the risk of unauthorized disclosure or modification of the applicable data. Requirement R2 covers implementation of the plan developed according to Requirement R1.

Questions

1. Requirement R1: The SDT drafted CIP-012-1 Requirement R1 for the Responsible Entity to develop one or more documented plan(s) to mitigate the risk of the unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring and control data while being transmitted between any Control Centers. Do you agree with this revision? If not, please provide the basis for your disagreement and an alternate proposal.

   ☐ Yes
   ☐ No

   Comments:

2. Requirement R1: The SDT seeks comment on scoping sensitive BES data as it applies to Real-time Assessment and Real-time monitoring and control data. Do you agree with scoping CIP-012-1 Requirement R1 in this manner? Please provide comment in support of your response.

   ☐ Yes
   ☐ No

   Comments:

3. Requirement R2: The SDT drafted CIP-012-1 Requirement R2 for the Responsible Entity to implement the plan(s) specified in Requirement R1, except under CIP Exceptional Circumstances. Do you agree with this revision? If not, please provide the basis for your disagreement and an alternate proposal.

   ☐ Yes
   ☐ No

   Comments:

4. Implementation Plan: The SDT revised the Implementation Plan to make the standard effective the first day of the first calendar quarter that is twenty-four (24) calendar months after the effective date of the applicable governmental authority's order approving the standard, or as otherwise provided for by the applicable governmental authority. Do you agree with this proposal? If you think an alternate implementation time period is needed, please provide a detailed explanation of actions and time needed to meet the implementation deadline.

   ☐ Yes
   ☐ No

   Comments:

5. The SDT believes proposed CIP-012-1 provides entities with flexibility to meet the reliability objectives in a cost effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost effective approaches, please provide your recommendation and, if appropriate, technical justification.

   ☐ Yes
   ☐ No

   Comments:

6. If you have additional comments on the proposed CIP-012-1 – Cyber Security – Communications between Control Centers drafted in response to the FERC directive that you have **not** provided in response to the questions above, please provide them here.

   Comments:

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Project 2016-02 Consideration of Issues and Directives

Federal Energy Regulatory Commission Order No. 822

October 27, 2017

Directives from FERC Order No. 822		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
53	53. As discussed in detail below, however, the Commission concludes that modifications to CIP-006-6 to provide controls to protect, at a minimum, communication links and data communicated between bulk electric system Control Centers are necessary in light of the critical role Control Center communications play in maintaining bulk electric system reliability. Therefore, we adopt the NOPR proposal and direct that NERC, pursuant to section 215(d)(5) of the FPA, develop modifications to the CIP Reliability Standards to require responsible entities to implement controls to protect, at a minimum, communication links and sensitive bulk electric system data communicated between bulk electric system Control Centers in a manner that is appropriately tailored to address the risks posed to the bulk electric system by the assets being protected (i.e., high, medium, or low impact).	The Project 2016-02 Standard Drafting Team (SDT) drafted Reliability Standard CIP-012-1 Requirement R1 to require responsible entities to document one or more plan(s) to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring and control data while being transmitted between Bulk Electric System (BES) Control Centers. Requirement R2 requires implementation of the documented plan(s). Due to the sensitivity of the data being transmitted between the Control Centers, the SDT created the standard to apply to all impact levels of BES Cyber Systems (i.e., high, medium, or low impact). Based on operational risk, the SDT determined that Real-time Assessments and Real-time monitoring and control data was the appropriate scope of the requirement. This critical information is necessary for immediate situational awareness and real-time operation of the BES.

Directives from FERC Order No. 822		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
		The SDT has drafted requirements allowing Responsible Entities the flexibility to apply protection to the communication links, the data, or both, consistent with their operational environments to satisfy the security objective of the Commission's directive FERC Order No. 822 specifically references CIP-006-6, which pertains to physical security controls. CIP-006-6, Requirement R1, Part 1.10 focuses on protecting the nonprogrammable communication components between Cyber Assets within the same ESP for medium and high impact BES Cyber Systems. The SDT asserts that most of the communications contemplated by FERC Order No. 822 are not within the same ESP, and, as such, CIP-006-6, Requirement R1, Part 1.10 would not be the appropriate location for this requirement.
54	54. NERC and other commenters recognize that inter-Control Center communications play a critical role in maintaining bulk electric system reliability by, among other things, helping to maintain situational awareness and reliable bulk electric system operations through timely and accurate communication between Control Centers.[59] We agree with this assessment. In order for certain responsible entities such as reliability coordinators, balancing authorities, and transmission operators to adequately perform their reliability	The SDT agrees that inter-Control Center communications play a critical role in Bulk Electric System reliability. Responsible Entities should therefore apply security measures to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring and control data. Since the current CIP Reliability Standards do not address this, the SDT has designed requirements to protect the data while it is being transmitted between inter-entity and intra-entity Control Centers.

Directives from FERC Order No. 822		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
	functions, their associated control centers must be capable of receiving and storing a variety of sensitive bulk electric system data from interconnected entities. Accordingly, we find that additional measures to protect both the integrity and availability of sensitive bulk electric system data are warranted.[60] We also understand that the attributes of the data managed by responsible entities could require different information protection controls. [61] For instance, certain types of reliability data will be sensitive to data manipulation type attacks, while other types of reliability data will be sensitive to eavesdropping type attacks aimed at collecting operational information (such as line and equipment ratings and impedances). NERC should consider the differing attributes of bulk electric system data as it assesses the development of appropriate controls. Footnotes: [59] NERC Comments at 20. [60] Protecting the integrity of bulk electric system data involves maintaining and ensuring the accuracy and consistency of inter-Control Center communications. Protecting the availability of bulk electric system data	The SDT has drafted requirements that allow responsible entities to apply protection to the communication links, the data, or both to satisfy the security objective consistent with the capabilities of the responsible entity's operational environment.

Directives from FERC Order No. 822		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
	involves ensuring that required data is available when needed for bulk electric system operations. [61] Moreover, in order for certain responsible entities to adequately perform their Reliability Functions, the associated control centers must be capable of receiving and storing a variety of sensitive data as specified by the IRO and TOP Standards. For instance, pursuant to Reliability Standard TOP-003-3, Requirements R1, R3 and R5, a transmission operator must maintain a documented specification for data and distribute its data specification to entities that have data required by the transmission operator's Operational Planning Analyses, Real-time Monitoring and Real-time Assessments. Entities receiving a data specification must satisfy the obligation of the documented specification.	
55	55. With regard to NERC's development of modifications responsive to our directive, we agree with NERC and other commenters that NERC should have flexibility in the manner in which it addresses the Commission's directive. Likewise, we find reasonable the principles outlined by NERC that protections for communication links and sensitive bulk electric system data communicated between bulk electric system Control Centers: (1) should not have an adverse effect on reliability, including the recognition of instances where	The SDT drafted Reliability Standard CIP-012-1 requirements to mitigate the risk of unauthorized disclosure or modification of Real-time Assessments and Real-time monitoring and control data while being transmitted between Control Centers. The SDT developed objective-based rather than prescriptive requirements. This approach will allow Responsible Entities flexibility in protecting these communications networks and sensitive BES data in a manner suited to each of their respective operational environments. It will also allow Responsible Entities to implement protection that considers the risks noted by the

Directives from FERC Order No. 822		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
	the introduction of latency could have negative results; (2) should account for the risk levels of assets and information being protected, and require protections that are commensurate with the risks presented; and (3) should be results-based in order to provide flexibility to account for the range of technologies and entities involved in bulk electric system communications.[62] Footnote: [62] See NERC Comments at 20-21.	Commission. The SDT identified a need to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring and control data regardless of asset risk level. The proposal requires protection for all Real-time Assessment and Real-time monitoring and control data while being transmitted between Control Centers.
56	56. We disagree with the assertion of NIPSCO and G&T Cooperatives that the risk posed by bulk electric system communication networks does not justify the costs of implementing controls. Communications between Control Centers over such networks are fundamental to the operations of the bulk electric system, and the record here does not persuade us that controls for such networks are not available at a reasonable cost (through encryption or otherwise). Nonetheless, we recognize that not all communication network components and data pose the same risk to bulk electric system reliability and may not require the same level of protection. We expect NERC to develop controls that reflect the risk posed by the asset or data being protected, and that can be implemented in	The SDT noted the FERC reference to additional Reliability Standards (TOP-003-3 and IRO-010-2) and the responsibilities to protect the data in accordance with those standards. The SDT interpreted these references as examples of potentially sensitive BES data and chose to base the CIP-012 requirements on the data specifications in TOP-003-3 and IRO-010-2.. This consolidates scoping and helps ensure that Responsible Entities mitigate the risk of the unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring and control data, rather than leaving the scoping of sensitive bulk electric system data to individual Responsible Entities. The SDT drafted CIP-012-1 to address confidentiality and integrity of Real-time Assessment and Real-time monitoring and control data. This was accomplished by drafting the

Directives from FERC Order No. 822		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
	a reasonable manner. It is important to recognize that certain entities are already required to exchange necessary real-time and operational planning data through secured networks using a "mutually agreeable security protocol," regardless of the entity's size or impact level.[63] 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. Footnote: [63] See Reliability Standards TOP-003-3, Requirement R5 and IRO-010-2, Requirement R3.	requirement to mitigate the risk from unauthorized disclosure or modification. The SDT asserts that the availability of this data is already required by the performance obligation of the TOP and IRO Reliability Standards. The SDT drafted CIP-012-1 to address the data while being transmitted. The SDT contends that this data is maintained within BES Cyber Systems, and is afforded the protections of CIP-003 through CIP-011 while at rest.
58	58. Several commenters sought clarification whether Control Centers owned by multiple registered entities would be included under the Commission's proposal. We clarify that the scope of the directed modifications apply to Control Center communications from facilities at all impact levels, regardless of ownership. The directed modification should encompass communication links and data for intra-Control Center and inter-Control Center communications.	The SDT drafted CIP-012-1 to apply to all impact levels of BES Cyber Systems (i.e., high, medium, or low impact), regardless of ownership. The SDT designed requirements to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring and control data while being transmitted between inter-entity and intra-entity BES Control Centers.

Directives from FERC Order No. 822		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
62	62. Several commenters addressed encryption and latency. Based on the record in this proceeding, it is reasonable to conclude that any lag in communication speed resulting from implementation of protections should only be measureable on the order of milliseconds and, therefore, will not adversely impact Control Center communications. Several commenters raise possible technical implementation difficulties with integrating encryption technologies into their current communications networks. Such technical issues should be considered by the standard drafting team when developing modifications in response to this directive, and may be resolved, e.g., by making certain aspects of the revised CIP Standards eligible for Technical Feasibility Exceptions.	The SDT developed objective-based rather than prescriptive requirements. This approach will allow Responsible Entities flexibility in mitigating the risk of unauthorized disclosure or modification of Real-time Assessments and Real-time monitoring data in a manner suited to each of their respective operational environments. It will also allow Responsible Entities to implement protection that considers the risks noted by the Commission.

Project 2016-02 Consideration of Issues and Directives

Federal Energy Regulatory Commission Order No. 822

~~June 21~~October 27, 2017

Directives from FERC Order No. 822		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
53	53. As discussed in detail below, however, the Commission concludes that modifications to CIP-006-6 to provide controls to protect, at a minimum, communication links and data communicated between bulk electric system Control Centers are necessary in light of the critical role Control Center communications play in maintaining bulk electric system reliability. Therefore, we adopt the NOPR proposal and direct that NERC, pursuant to section 215(d)(5) of the FPA, develop modifications to the CIP Reliability Standards to require responsible entities to implement controls to protect, at a minimum, communication links and sensitive bulk electric system data communicated between bulk electric system Control Centers in a manner that is appropriately tailored to address the risks posed to the bulk electric system by the assets being protected (i.e., high, medium, or low impact).	The Project 2016-02 Standard Drafting Team (SDT) drafted Reliability Standard CIP-012-1 Requirement R1 to require responsible entities to document one or more plan(s) to mitigate the risk of ~~the~~ unauthorized disclosure or modification of ~~data used for Operational Planning Analysis,~~ Real-time ~~Assessments,~~Assessment and Real-time monitoring and control data while being transmitted between Bulk Electric System (BES) Control Centers. Requirement R2 requires implementation of the documented plan(s). Due to the sensitivity of the data being transmitted between the Control Centers, ~~as defined in the NERC Glossary of Terms Used in Reliability Standards,~~ the SDT created the standard ~~and determined that it applies~~to apply to all impact levels of BES Cyber Systems (i.e., high, medium, or low impact). Based on operational risk, the SDT determined that Real-time Assessments and Real-time monitoring and control data was the appropriate scope of the requirement. This critical

Directives from FERC Order No. 822		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
		information is necessary for immediate situational awareness and real-time operation of the BES. The SDT has drafted requirements allowing Responsible Entities the flexibility to apply protection to the communication links, the data, or both, consistent with their operational environments to satisfy the security objective of the Commission's directive~~, consistent with the capabilities of the Responsible Entity's operational environment. The directive language~~ FERC Order No. 822 specifically references CIP-006-6, which pertains to physical security controls. CIP-006-6, Requirement R1, Part 1.10 focuses on protecting the nonprogrammable communication components between Cyber Assets within the same ESP for medium and high impact BES Cyber Systems. The SDT asserts that most of the communications contemplated by ~~the~~FERC Order No. 822 are not within the same ESP, and ~~that~~, as such, CIP-006-6, Requirement R1, Part 1.10 would not be the appropriate location for this requirement.
54	54. NERC and other commenters recognize that inter-Control Center communications play a critical role in maintaining bulk electric system reliability by, among other things, helping to maintain situational awareness and reliable bulk electric system operations through	The SDT agrees that inter-Control Center communications play a critical role in Bulk Electric System reliability. Responsible Entities should therefore apply security measures to mitigate the risk of ~~the~~ unauthorized disclosure or modification of ~~data used for Operational Planning Analysis,~~ Real-time

Directives from FERC Order No. 822		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
	timely and accurate communication between Control Centers.[59] We agree with this assessment. In order for certain responsible entities such as reliability coordinators, balancing authorities, and transmission operators to adequately perform their reliability functions, their associated control centers must be capable of receiving and storing a variety of sensitive bulk electric system data from interconnected entities. Accordingly, we find that additional measures to protect both the integrity and availability of sensitive bulk electric system data are warranted.[60] We also understand that the attributes of the data managed by responsible entities could require different information protection controls. [61] For instance, certain types of reliability data will be sensitive to data manipulation type attacks, while other types of reliability data will be sensitive to eavesdropping type attacks aimed at collecting operational information (such as line and equipment ratings and impedances). NERC should consider the differing attributes of bulk electric system data as it assesses the development of appropriate controls. Footnotes: [59] NERC Comments at 20.	~~Assessments,~~Assessment and Real-time monitoring~~, which~~ and control data. Since the current CIP Reliability Standards do not address~~. As such~~ this, the SDT has ~~defined~~designed requirements ~~that are designed~~ to protect the data while it is being transmitted between inter-entity and intra-entity Control Centers. The SDT has drafted requirements ~~allowing~~that allow responsible entities to apply protection to the communication links, the data, or both to satisfy the security objective consistent with the capabilities of –the responsible entity's operational environment.

Directives from FERC Order No. 822		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
	[60] Protecting the integrity of bulk electric system data involves maintaining and ensuring the accuracy and consistency of inter-Control Center communications. Protecting the availability of bulk electric system data involves ensuring that required data is available when needed for bulk electric system operations. [61] Moreover, in order for certain responsible entities to adequately perform their Reliability Functions, the associated control centers must be capable of receiving and storing a variety of sensitive data as specified by the IRO and TOP Standards. For instance, pursuant to Reliability Standard TOP-003-3, Requirements R1, R3 and R5, a transmission operator must maintain a documented specification for data and distribute its data specification to entities that have data required by the transmission operator's Operational Planning Analyses, Real-time Monitoring and Real-time Assessments. Entities receiving a data specification must satisfy the obligation of the documented specification.	
55	55. With regard to NERC's development of modifications responsive to our directive, we agree with NERC and other commenters that NERC should have flexibility in the manner in which it addresses the Commission's directive. Likewise, we find reasonable the principles outlined by NERC that protections for communication	The SDT drafted Reliability Standard CIP-012-1 ~~to establish~~ requirements to mitigate the risk of ~~the~~ unauthorized disclosure or modification of ~~data used for Operational Planning Analysis,~~ Real-time Assessments~~,~~ and Real-time monitoring and control data while being transmitted between Control Centers. The SDT developed objective-based rather than prescriptive

Directives from FERC Order No. 822		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
	links and sensitive bulk electric system data communicated between bulk electric system Control Centers: (1) should not have an adverse effect on reliability, including the recognition of instances where the introduction of latency could have negative results; (2) should account for the risk levels of assets and information being protected, and require protections that are commensurate with the risks presented; and (3) should be results-based in order to provide flexibility to account for the range of technologies and entities involved in bulk electric system communications.[62] Footnote: [62] See NERC Comments at 20-21.	requirements. This approach will allow Responsible Entities flexibility in protecting these communications networks and sensitive BES data in a manner suited to each of their respective operational environments. It will also allow Responsible Entities to implement protection that considers the risks noted by the Commission. The SDT identified a need to mitigate the risk of ~~the~~ unauthorized disclosure or modification of ~~data used for Operational Planning Analysis,~~ Real-time Assessment~~,~~ and Real-time monitoring and control data regardless of asset risk level. The proposal requires protection for all ~~data used for Operational Planning Analysis,~~ Real-time Assessment~~,~~ and Real-time monitoring and control data while being transmitted between Control Centers.
56	56. We disagree with the assertion of NIPSCO and G&T Cooperatives that the risk posed by bulk electric system communication networks does not justify the costs of implementing controls. Communications between Control Centers over such networks are fundamental to the operations of the bulk electric system, and the record here does not persuade us that controls for such networks are not available at a reasonable cost (through encryption or otherwise). Nonetheless, we recognize that not all communication network components and data pose the same risk to	The SDT noted the FERC reference to additional Reliability Standards (TOP-003-3 and IRO-010-2) and the responsibilities to protect the data in accordance with those standards ~~(TOP-003-3 and IRO-010-2).~~. The SDT interpreted these references as examples of potentially sensitive BES data and chose to base the CIP-012 requirements on the data specifications in ~~these standards.~~TOP-003-3 and IRO-010-2.. This consolidates scoping and helps ensure that Responsible Entities mitigate the risk of the unauthorized disclosure or modification of ~~Operational Planning Analysis,~~ Real-time Assessment~~,~~ and Real-time monitoring and control data, rather than leaving the scoping of

Directives from FERC Order No. 822		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
	bulk electric system reliability and may not require the same level of protection. We expect NERC to develop controls that reflect the risk posed by the asset or data being protected, and that can be implemented in a reasonable manner. It is important to recognize that certain entities are already required to exchange necessary real-time and operational planning data through secured networks using a "mutually agreeable security protocol," regardless of the entity's size or impact level.[63] 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. Footnote: [63] See Reliability Standards TOP-003-3, Requirement R5 and IRO-010-2, Requirement R3.	sensitive bulk electric system data to individual Responsible Entities. The SDT drafted CIP-012-1 to address confidentiality and integrity of ~~data used for Operational Planning Analysis,~~ Real-time Assessment~~,~~ and Real-time monitoring~~. These are accommodated~~ and control data. This was accomplished by drafting the requirement to mitigate the risk from unauthorized disclosure or modification. The SDT ~~contends~~asserts that the availability of this data is already required by the performance obligation of the ~~Operating~~TOP and ~~Planning~~IRO Reliability Standards. The SDT drafted CIP-012-1 to address the data while being transmitted. The SDT contends that this data is maintained within BES Cyber Systems, and is afforded the protections of CIP-003 through CIP-011~~.~~ while at rest.
58	58. Several commenters sought clarification whether Control Centers owned by multiple registered entities would be included under the Commission's proposal. We clarify that the scope of the directed modifications apply to Control Center communications from	The SDT ~~created the standard and determined that it applies~~drafted CIP-012-1 to apply to all impact levels of BES Cyber Systems (i.e., high, medium, or low impact), regardless of ownership. The SDT ~~defined~~designed requirements ~~that are designed~~ to mitigate the risk of ~~the~~ unauthorized disclosure or

Directives from FERC Order No. 822		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
	facilities at all impact levels, regardless of ownership. The directed modification should encompass communication links and data for intra-Control Center and inter-Control Center communications.	modification of ~~data used for Operational Planning Analysis,~~ Real-time Assessment~~,~~ and Real-time monitoring and control data while being transmitted between inter-entity and intra-entity BES Control Centers.
62	62. Several commenters addressed encryption and latency. Based on the record in this proceeding, it is reasonable to conclude that any lag in communication speed resulting from implementation of protections should only be measureable on the order of milliseconds and, therefore, will not adversely impact Control Center communications. Several commenters raise possible technical implementation difficulties with integrating encryption technologies into their current communications networks. Such technical issues should be considered by the standard drafting team when developing modifications in response to this directive, and may be resolved, e.g., by making certain aspects of the revised CIP Standards eligible for Technical Feasibility Exceptions.	The SDT developed objective-based rather than prescriptive requirements. This approach will allow Responsible Entities flexibility in mitigating the risk of ~~the~~ unauthorized disclosure or modification of ~~data used for Operational Planning Analysis,~~ Real-time Assessments~~,~~ and Real-time monitoring data in a manner suited to each of their respective operational environments. It will also allow Responsible Entities to implement protection that considers the risks noted by the Commission.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Violation Risk Factor and Violation Severity Level Justifications

Project 2016-02 Modifications to CIP Standards

This document provides the standard drafting team's (SDT's) justification for assignment of violation risk factors (VRFs) and violation severity levels (VSLs) for each requirement in **CIP-012-1**. Each requirement is assigned a VRF and a VSL. These elements support the determination of an initial value range for the Base Penalty Amount regarding violations of requirements in FERC-approved Reliability Standards, as defined in the Electric Reliability Organizations (ERO) Sanction Guidelines. The SDT applied the following NERC criteria and FERC Guidelines when developing the VRFs and VSLs for the requirements.

NERC Criteria for Violation Risk Factors

High Risk Requirement

A requirement that, if violated, could directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures, or could hinder restoration to a normal condition.

Medium Risk Requirement

A requirement that, if violated, could directly affect the electrical state or the capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System. However, violation of a medium risk requirement is unlikely to lead to Bulk Electric System instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System. However, violation of a medium risk requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to Bulk Electric System instability, separation, or cascading failures, nor to hinder restoration to a normal condition.

Lower Risk Requirement

A requirement that is administrative in nature and a requirement that, if violated, would not be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System; or, a requirement that is administrative in nature and a requirement in a planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.

FERC Guidelines for Violation Risk Factors

Guideline (1) – Consistency with the Conclusions of the Final Blackout Report

FERC seeks to ensure that VRFs assigned to Requirements of Reliability Standards in these identified areas appropriately reflect their historical critical impact on the reliability of the Bulk-Power System. In the VSL Order, FERC listed critical areas (from the Final Blackout Report) where violations could severely affect the reliability of the Bulk-Power System:

- Emergency operations
- Vegetation management
- Operator personnel training
- Protection systems and their coordination
- Operating tools and backup facilities
- Reactive power and voltage control
- System modeling and data exchange
- Communication protocol and facilities
- Requirements to determine equipment ratings
- Synchronized data recorders
- Clearer criteria for operationally critical facilities
- Appropriate use of transmission loading relief.

Guideline (2) – Consistency within a Reliability Standard

FERC expects a rational connection between the sub-Requirement VRF assignments and the main Requirement VRF assignment.

Guideline (3) – Consistency among Reliability Standards

FERC expects the assignment of VRFs corresponding to Requirements that address similar reliability goals in different Reliability Standards would be treated comparably.

Guideline (4) – Consistency with NERC's Definition of the Violation Risk Factor Level

Guideline (4) was developed to evaluate whether the assignment of a particular VRF level conforms to NERC's definition of that risk level.

Guideline (5) – Treatment of Requirements that Co-mingle More Than One Obligation

Where a single Requirement co-mingles a higher risk reliability objective and a lesser risk reliability objective, the VRF assignment for such Requirements must not be watered down to reflect the lower risk level associated with the less important objective of the Reliability Standard.

NERC Criteria for Violation Severity Levels

VSLs define the degree to which compliance with a requirement was not achieved. Each requirement must have at least one VSL. While it is preferable to have four VSLs for each requirement, some requirements do not have multiple "degrees" of noncompliant performance and may have only one, two, or three VSLs.

VSLs should be based on NERC's overarching criteria shown in the table below:

Lower VSL	Moderate VSL	High VSL	Severe VSL
The performance or product measured almost meets the full intent of the requirement.	The performance or product measured meets the majority of the intent of the requirement.	The performance or product measured does not meet the majority of the intent of the requirement, but does meet some of the intent.	The performance or product measured does not substantively meet the intent of the requirement.

FERC Order of Violation Severity Levels

The FERC VSL guidelines are presented below, followed by an analysis of whether the VSLs proposed for each requirement in the standard meet the FERC Guidelines for assessing VSLs:

Guideline (1) – Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance

Compare the VSLs to any prior levels of non-compliance and avoid significant changes that may encourage a lower level of compliance than was required when levels of non-compliance were used.

Guideline (2) – Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties

A violation of a "binary" type requirement must be a "Severe" VSL.

Do not use ambiguous terms such as "minor" and "significant" to describe noncompliant performance.

Guideline (3) – Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement

VSLs should not expand on what is required in the requirement.

Guideline (4) – Violation Severity Level Assignment Should Be Based on a Single Violation, Not on a Cumulative Number of Violations

Unless otherwise stated in the requirement, each instance of non-compliance with a requirement is a separate violation. Section 4 of the Sanction Guidelines states that assessing penalties on a per violation per day basis is the "default" for penalty calculations.

VRF Justifications for CIP-012-1, Requirement R1	
Proposed VRF	**Medium**
NERC VRF Discussion	A VRF of Medium was assigned to this requirement. Cyber security plans enable effective implementation of the CIP standard's requirements to mitigate the risk of the unauthorized disclosure or modification of data used for Operational Planning Analysis, Real-time Assessments, and Real-time monitoring while being transmitted between Control Centers.
FERC VRF G1 Discussion Guideline 1- Consistency with Blackout Report	N/A
FERC VRF G2 Discussion Guideline 2- Consistency within a Reliability Standard	N/A
FERC VRF G3 Discussion Guideline 3- Consistency among Reliability Standards	The requirement complements CIP-005-1, Requirement R1, CIP-006-6, Requirement R1, and CIP-007-6, Requirement R1 which are related to security of networks and communications components. The proposed VRF is consistent with these related requirements.
FERC VRF G4 Discussion Guideline 4- Consistency with NERC Definitions of VRFs	Failure to have a cyber security plan would not, under Emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.
FERC VRF G5 Discussion	N/A

VRF Justifications for CIP-012-1, Requirement R1	
Proposed VRF	**Medium**
Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation	

VSLs for CIP-012-1, Requirement R1			
Lower	**Moderate**	**High**	**Severe**
N/A	The Responsible Entity documented its plan(s) but failed to include one of the applicable parts of the plan as specified in Requirement R1.	The Responsible Entity documented its plan(s) but failed to include two of the applicable parts of the plan as specified in Requirement R1.	The Responsible Entity failed to document plan(s) for Requirement R1.

VSL Justifications for CIP-012-1 Requirements R1	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The requirement is new. Therefore, the proposed VSL does not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The requirement is for the Responsible Entity to document include one or more plans as specified in Requirement R1. The moderate VSL addresses where the Responsible Entity documented its plan(s) but failed to include one of the applicable parts of the plan as specified in Requirement R1. The high VSL addresses where the Responsible Entity documented its plan(s) but failed to include two of the applicable parts of the plan as specified in Requirement R1. The severe VSL addresses where the Responsible Entity failed to document plan(s) for Requirement R1.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL uses the same terminology as used in the associated requirement and is, therefore, consistent with the requirement.

FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Each VSL is based on a single violation and not cumulative violations.

VRF Justifications for CIP-012-1, Requirement R2	
Proposed VRF	**Medium**
NERC VRF Discussion	A VRF of Medium was assigned to this requirement. Implementation of required cyber security plans enable effective implementation of the CIP standard's requirements to mitigate the risk of the unauthorized disclosure or modification of data used for Operational Planning Analysis, Real-time Assessments, and Real-time monitoring while being transmitted between Control Centers.
FERC VRF G1 Discussion Guideline 1- Consistency with Blackout Report	N/A
FERC VRF G2 Discussion Guideline 2- Consistency within a Reliability Standard	N/A
FERC VRF G3 Discussion Guideline 3- Consistency among Reliability Standards	The requirement complements CIP-005-1, Requirement R1, CIP-006-6, Requirement R1, and CIP-007-6, Requirement R1 which are related to security of networks and communications components. The proposed VRF is consistent with these related requirements.
FERC VRF G4 Discussion	Failure to properly implement the cyber security plan would not, under Emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state

VRF Justifications for CIP-012-1, Requirement R2	
Proposed VRF	**Medium**
Guideline 4- Consistency with NERC Definitions of VRFs	or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.
FERC VRF G5 Discussion Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation	N/A

VSLs for CIP-012-1, Requirement R2			
Lower	**Moderate**	**High**	**Severe**
N/A	N/A	N/A	The Responsible Entity failed to implement its plan(s) as specified in Requirement R1, except under CIP Exceptional Circumstances.

VSL Justifications for CIP-012-1 Requirement R2	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The requirement is new. Therefore, the proposed VSL does not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSL is binary and is classified as severe. The VSL does not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL uses the same terminology as used in the associated requirement and is, therefore, consistent with the requirement.

FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSL is based on a single violation and not cumulative violations.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Violation Risk Factor and Violation Severity Level Justifications

Project 2016-02 Modifications to CIP Standards

This document provides the standard drafting team's (SDT's) justification for assignment of violation risk factors (VRFs) and violation severity levels (VSLs) for each requirement in **CIP-012-1**. Each requirement is assigned a VRF and a VSL. These elements support the determination of an initial value range for the Base Penalty Amount regarding violations of requirements in FERC-approved Reliability Standards, as defined in the Electric Reliability Organizations (ERO) Sanction Guidelines. The SDT applied the following NERC criteria and FERC Guidelines when developing the VRFs and VSLs for the requirements.

NERC Criteria for Violation Risk Factors

High Risk Requirement

A requirement that, if violated, could directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures, or could hinder restoration to a normal condition.

Medium Risk Requirement

A requirement that, if violated, could directly affect the electrical state or the capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System. However, violation of a medium risk requirement is unlikely to lead to Bulk Electric System instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System. However, violation of a medium risk requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to Bulk Electric System instability, separation, or cascading failures, nor to hinder restoration to a normal condition.

Lower Risk Requirement
A requirement that is administrative in nature and a requirement that, if violated, would not be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System; or, a requirement that is administrative in nature and a requirement in a planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.

FERC Guidelines for Violation Risk Factors

Guideline (1) – Consistency with the Conclusions of the Final Blackout Report

FERC seeks to ensure that VRFs assigned to Requirements of Reliability Standards in these identified areas appropriately reflect their historical critical impact on the reliability of the Bulk-Power System. In the VSL Order, FERC listed critical areas (from the Final Blackout Report) where violations could severely affect the reliability of the Bulk-Power System:

- Emergency operations
- Vegetation management
- Operator personnel training
- Protection systems and their coordination
- Operating tools and backup facilities
- Reactive power and voltage control
- System modeling and data exchange
- Communication protocol and facilities
- Requirements to determine equipment ratings
- Synchronized data recorders
- Clearer criteria for operationally critical facilities
- Appropriate use of transmission loading relief.

Guideline (2) – Consistency within a Reliability Standard

FERC expects a rational connection between the sub-Requirement VRF assignments and the main Requirement VRF assignment.

Guideline (3) – Consistency among Reliability Standards

FERC expects the assignment of VRFs corresponding to Requirements that address similar reliability goals in different Reliability Standards would be treated comparably.

Guideline (4) – Consistency with NERC's Definition of the Violation Risk Factor Level

Guideline (4) was developed to evaluate whether the assignment of a particular VRF level conforms to NERC's definition of that risk level.

Guideline (5) – Treatment of Requirements that Co-mingle More Than One Obligation

Where a single Requirement co-mingles a higher risk reliability objective and a lesser risk reliability objective, the VRF assignment for such Requirements must not be watered down to reflect the lower risk level associated with the less important objective of the Reliability Standard.

NERC Criteria for Violation Severity Levels

VSLs define the degree to which compliance with a requirement was not achieved. Each requirement must have at least one VSL. While it is preferable to have four VSLs for each requirement, some requirements do not have multiple "degrees" of noncompliant performance and may have only one, two, or three VSLs.

VSLs should be based on NERC's overarching criteria shown in the table below:

Lower VSL	Moderate VSL	High VSL	Severe VSL
The performance or product measured almost meets the full intent of the requirement.	The performance or product measured meets the majority of the intent of the requirement.	The performance or product measured does not meet the majority of the intent of the requirement, but does meet some of the intent.	The performance or product measured does not substantively meet the intent of the requirement.

FERC Order of Violation Severity Levels

The FERC VSL guidelines are presented below, followed by an analysis of whether the VSLs proposed for each requirement in the standard meet the FERC Guidelines for assessing VSLs:

Guideline (1) – Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance

Compare the VSLs to any prior levels of non-compliance and avoid significant changes that may encourage a lower level of compliance than was required when levels of non-compliance were used.

Guideline (2) – Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties

A violation of a "binary" type requirement must be a "Severe" VSL.

Do not use ambiguous terms such as "minor" and "significant" to describe noncompliant performance.

Guideline (3) – Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement

VSLs should not expand on what is required in the requirement.

Guideline (4) – Violation Severity Level Assignment Should Be Based on a Single Violation, Not on a Cumulative Number of Violations

Unless otherwise stated in the requirement, each instance of non-compliance with a requirement is a separate violation. Section 4 of the Sanction Guidelines states that assessing penalties on a per violation per day basis is the "default" for penalty calculations.

VRF Justifications for CIP-012-1, Requirement R1	
Proposed VRF	**Medium**
NERC VRF Discussion	A VRF of Medium was assigned to this requirement. Cyber security plans enable effective implementation of the CIP standard's requirements to mitigate the risk of the unauthorized disclosure or modification of data used for Operational Planning Analysis, Real-time Assessments, and Real-time monitoring while being transmitted between Control Centers.
FERC VRF G1 Discussion Guideline 1- Consistency with Blackout Report	N/A
FERC VRF G2 Discussion Guideline 2- Consistency within a Reliability Standard	N/A
FERC VRF G3 Discussion Guideline 3- Consistency among Reliability Standards	The requirement complements CIP-005-1, Requirement R1, CIP-006-6, Requirement R1, and CIP-007-6, Requirement R1 which are related to security of networks and communications components. The proposed VRF is consistent with these related requirements.
FERC VRF G4 Discussion Guideline 4- Consistency with NERC Definitions of VRFs	Failure to have a cyber security plan would not, under Emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.
FERC VRF G5 Discussion	N/A

VRF Justifications for CIP-012-1, Requirement R1	
Proposed VRF	**Medium**
Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation	

VSLs for CIP-012-1, Requirement R1			
Lower	**Moderate**	**High**	**Severe**
N/A	~~N/A~~ The Responsible Entity documented its plan(s) but failed to include one of the applicable parts of the plan as specified in Requirement R1.	~~N/A~~The Responsible Entity documented its plan(s) but failed to include two of the applicable parts of the plan as specified in Requirement R1.	The Responsible Entity failed to document ~~one or more~~ plan(s) ~~that achieve the security objective to mitigate the risk of the unauthorized disclosure or modification of data used~~ for ~~Operational Planning Analysis, Real-time Assessments, and Real-time monitoring while being transmitted, excluding oral communication, between Controls Centers as specified in~~ Requirement R1.

VSL Justifications for CIP-012-1 Requirements R1	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The requirement is new. Therefore, the proposed VSL does not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	~~The proposed VSL is binary and is classified as severe. The VSL does not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.~~The requirement is for the Responsible Entity to document include one or more plans as specified in Requirement R1. The moderate VSL addresses where the Responsible Entity documented its plan(s) but failed to include one of the applicable parts of the plan as specified in Requirement R1. The high VSL addresses where the Responsible Entity documented its plan(s) but failed to include two of the applicable parts of the plan as specified in Requirement R1. The severe VSL addresses where the Responsible Entity failed to document plan(s) for Requirement R1.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL uses the same terminology as used in the associated requirement and is, therefore, consistent with the requirement.

FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	~~The~~Each VSL is based on a single violation and not cumulative violations.

VRF Justifications for CIP-012-1, Requirement R2	
Proposed VRF	**Medium**
NERC VRF Discussion	A VRF of Medium was assigned to this requirement. Implementation of required cyber security plans enable effective implementation of the CIP standard's requirements to mitigate the risk of the unauthorized disclosure or modification of data used for Operational Planning Analysis, Real-time Assessments, and Real-time monitoring while being transmitted between Control Centers.
FERC VRF G1 Discussion Guideline 1- Consistency with Blackout Report	N/A
FERC VRF G2 Discussion Guideline 2- Consistency within a Reliability Standard	N/A
FERC VRF G3 Discussion Guideline 3- Consistency among Reliability Standards	The requirement complements CIP-005-1, Requirement R1, CIP-006-6, Requirement R1, and CIP-007-6, Requirement R1 which are related to security of networks and communications components. The proposed VRF is consistent with these related requirements.
FERC VRF G4 Discussion	Failure to properly implement the cyber security plan would not, under Emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state

VRF Justifications for CIP-012-1, Requirement R2	
Proposed VRF	**Medium**
Guideline 4- Consistency with NERC Definitions of VRFs	or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.
FERC VRF G5 Discussion Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation	N/A

VSLs for CIP-012-1, Requirement R2			
Lower	**Moderate**	**High**	**Severe**
N/A	N/A	N/A	The Responsible Entity failed to implement its plan ~~to mitigate the risk of the unauthorized disclosure or modification of data used for Operational, Planning Analysis, Real-time Assessments, and Real-time monitoring while being transmitted, excluding oral communication, between Controls Centers~~(s) as specified in Requirement R1, except under CIP Exceptional Circumstances.

VSL Justifications for CIP-012-1 Requirement R2	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The requirement is new. Therefore, the proposed VSL does not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSL is binary and is classified as severe. The VSL does not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL uses the same terminology as used in the associated requirement and is, therefore, consistent with the requirement.

FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSL is based on a single violation and not cumulative violations.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Reliability Standard Audit Worksheet[1]

CIP-012-1 – Cyber Security – Communications between Control Centers

This section to be completed by the Compliance Enforcement Authority.

Audit ID:	Audit ID if available; or REG-NCRnnnnn-YYYYMMDD
Registered Entity:	Registered name of entity being audited
NCR Number:	NCRnnnnn
Compliance Enforcement Authority:	Region or NERC performing audit
Compliance Assessment Date(s)[2]:	Month DD, YYYY, to Month DD, YYYY
Compliance Monitoring Method:	[On-site Audit | Off-site Audit | Spot Check]
Names of Auditors:	Supplied by CEA

Applicability of Requirements

	BA	DP	GO	GOP	PA/PC	RC	RP	RSG	TO	TOP	TP	TSP
R1	X		X	X		X			X	X		
R2	X		X	X		X			X	X		

Legend:

Text with blue background:	Fixed text – do not edit
Text entry area with Green background:	Entity-supplied information
Text entry area with white background:	Auditor-supplied information

[1] NERC developed this Reliability Standard Audit Worksheet (RSAW) language in order to facilitate NERC's and the Regional Entities' assessment of a registered entity's compliance with this Reliability Standard. The NERC RSAW language is written to specific versions of each NERC Reliability Standard. Entities using this RSAW should choose the version of the RSAW applicable to the Reliability Standard being assessed. While the information included in this RSAW provides some of the methodology that NERC has elected to use to assess compliance with the requirements of the Reliability Standard, this document should not be treated as a substitute for the Reliability Standard or viewed as additional Reliability Standard requirements. In all cases, the Regional Entity should rely on the language contained in the Reliability Standard itself, and not on the language contained in this RSAW, to determine compliance with the Reliability Standard. NERC's Reliability Standards can be found on NERC's website. Additionally, NERC Reliability Standards are updated frequently, and this RSAW may not necessarily be updated with the same frequency. Therefore, it is imperative that entities treat this RSAW as a reference document only, and not as a substitute or replacement for the Reliability Standard. It is the responsibility of the registered entity to verify its compliance with the latest approved version of the Reliability Standards, by the applicable governmental authority, relevant to its registration status.

The RSAW may provide a non-exclusive list, for informational purposes only, of examples of the types of evidence a registered entity may produce or may be asked to produce to demonstrate compliance with the Reliability Standard. A registered entity's adherence to the examples contained within this RSAW does not necessarily constitute compliance with the applicable Reliability Standard, and NERC and the Regional Entity using this RSAW reserve the right to request additional evidence from the registered entity that is not included in this RSAW. This RSAW may include excerpts from FERC Orders and other regulatory references which are provided for ease of reference only, and this document does not necessarily include all applicable Order provisions. In the event of a discrepancy between FERC Orders, and the language included in this document, FERC Orders shall prevail.

[2] Compliance Assessment Date(s): The date(s) the actual compliance assessment (on-site audit, off-site spot check, etc.) occurs.

Findings

(This section to be completed by the Compliance Enforcement Authority)

Req.	Finding	Summary and Documentation	Functions Monitored
R1			
R2			

Req.	Areas of Concern

Req.	Recommendations

Req.	Positive Observations

Subject Matter Experts

Identify the Subject Matter Expert(s) responsible for this Reliability Standard.

Registered Entity Response (Required; Insert additional rows if needed):

SME Name	Title	Organization	Requirement(s)

Registered Entity Response (Required):

Question 1: Does the Registered Entity own or operate a Control Center? ☐ Yes ☐ No

If no:

1. Provide evidence in the space that the Registered Entity does not own or operate one or more Control Centers. This evidence may include, but is not limited to:
   - Evidence that the Registered Entity does not own or operate a Control Center; or
   - Evidence or a reference to evidence from the Registered Entity's CIP-002 compliance program that demonstrates the entity does not own or operate a Control Center.
2. The remainder of this RSAW may be left blank.

[Note: A separate spreadsheet or other document may be used. If so, provide the document reference below.]

R1 Supporting Evidence and Documentation

R1. The Responsible Entity shall develop one or more documented plan(s) to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring and control data while being transmitted between any Control Centers. This requirement excludes oral communications. The plan shall include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

- **1.1** Identification of security protection used to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring and control data while being transmitted between Control Centers;
- **1.2** Identification of demarcation point(s) where security protection is applied for transmitting Real-time Assessment and Real-time monitoring and control data between Control Centers; and
- **1.3** Identification of roles and responsibilities of each Responsible Entity for applying security protection to the transmission of Real-time Assessment and Real-time monitoring and control data between Control Centers, when the Control Centers are owned or operated by different Responsible Entities.

M1. Evidence may include, but is not limited to, documented plan(s) that meet the security objective of Requirement R1.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-012-1, R1

This section to be completed by the Compliance Enforcement Authority

	If the Registered Entity has answered "No" to Question 1, verify the Registered Entity does not own or operate a Control Center. Note: If the Registered Entity does not own or operate a Control Center, the remainder of this RSAW is not applicable.
	Verify the entity has developed one or more documented plan(s) to mitigate the risk of the unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring and control data while being transmitted between Control Centers.
	Verify the documented plans collectively include identification of security protection used to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring and control data while being transmitted between Control Centers.
	Verify the documented plans collectively include identification of demarcation point(s) where security protection is applied for transmitting Real-time Assessment and Real-time monitoring and control data between Control Centers.
	Verify the documented plans collectively include identification of roles and responsibilities of each Responsible Entity for applying security protection to the transmission of Real-time Assessment and Real-time monitoring and control data between Control Centers, when the Control Centers are owned or operated by different Responsible Entities.
	Verify the documented plans collectively achieve the security objective of mitigating the risk of the unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring and control data while being transmitted between Control Centers.
Note to Auditor: 1. Oral communications are not in scope for CIP-012-1.	

Auditor Notes:

R2 Supporting Evidence and Documentation

R2. The Responsible Entity shall implement the plan(s) specified in Requirement R1, except under CIP Exceptional Circumstances.

M2. Evidence may include, but is not limited to, documentation to demonstrate implementation of methods to mitigate the risk of the unauthorized disclosure or modification of data in Requirement R1.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-012-1, R2

This section to be completed by the Compliance Enforcement Authority

	Verify the entity has implemented one or more documented plan(s) to mitigate the risk of the unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring and control data while being transmitted between Control Centers.
	Verify the entity has implemented the identified security protection used to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring and control data while being transmitted between Control Centers.
	Verify the entity has implemented the identified security protection at the identified demarcation point(s) where security protection is applied for transmitting Real-time Assessment and Real-time monitoring and control data between Control Centers; and
	If Control Centers are not owned and operated by the same Responsible Entity, verify the entity has identified roles and responsibilities of each Responsible Entity for applying security protection to the transmission of Real-time Assessment and Real-time monitoring and control data between Control Centers.
	If the Responsible Entity has declared and responded to CIP Exceptional Circumstances, verify the Responsible Entity has adhered to the applicable cyber security policies.
Note to Auditor: The Responsible Entity may reference a separate set of documents to demonstrate its response to any requirements impacted by CIP Exceptional Circumstances.	

Auditor Notes:

Additional Information:

Reliability Standard

The full text of CIP-012-1 may be found on the NERC Web Site (www.nerc.com) under "Program Areas & Departments", "Standards," "Reliability Standards."

In addition to the Reliability Standard, there is an applicable Implementation Plan available on the NERC Web Site.

In addition to the Reliability Standard, there is background information available on the NERC Web Site.

Capitalized terms in the Reliability Standard refer to terms in the NERC Glossary, which may be found on the NERC Web Site.

Sampling Methodology

Sampling is essential for auditing compliance with NERC Reliability Standards since it is not always possible or practical to test 100% of either the equipment, documentation, or both, associated with the full suite of enforceable standards. The Sampling Methodology Guidelines and Criteria (see NERC website), or sample guidelines, provided by the Electric Reliability Organization help to establish a minimum sample set for monitoring and enforcement uses in audits of NERC Reliability Standards.

Regulatory Language

FERC Order 822 P53-56, 58, and 62

Selected Glossary Terms

The following Glossary terms are provided for convenience only. Please refer to the NERC web site for the current enforceable terms.

CIP Exceptional Circumstance

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.

Control Center

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, of: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for transmission Facilities at two or more locations, or 4) a Generator Operator for generation Facilities at two or more locations.

Real-time Assessment

An evaluation of system conditions using Real-time data to assess existing (pre-Contingency) and potential (post-Contingency) operating conditions. The assessment shall reflect applicable inputs including, but not limited to: load, generation output levels, known Protection System and Special Protection System status or degradation, Transmission outages, generator outages, Interchange, Facility Ratings, and identified phase angle and equipment limitations. (Real-time Assessment may be provided through internal systems or through third-party services.)

Real-time
Present time as opposed to future time.

Revision History for RSAW

Version	Date	Reviewers	Revision Description
Draft1 v1	07/28/2017	NERC Stds Group	New document
Draft1 v2	08/01/2017	RSAW Task Force	Modified Question to clarify applicability
Draft1 v3	08/02/2017	RSAW Task Force	Response to MRO comments. Moved Questions 1 and 2 above R1. Made text changes to Q1 and to R2 Compliance Assessment Approach.
Draft1 v4	08/07/2017	RSAW Task Force, 2016-02 SDT	Response to TexasRE and SDT comments. Clarified scope of Q1 to be data transmitted between Control Centers. Removed extra space from Auditor Notes.
Draft2 v1	10/27/2017	RSAW Task Force	Modified title. Modified Q2 to conform with new language. Modified R1 with new Requirement text and new Compliance Assessment Approach. Modified R2 with new Compliance Assessment Approach. Removed Operational Planning Analysis from the Selected Glossary Terms. Modified footer with revised version and date.
Draft2 v2	11/27/2017	RSAW Task Force, Standard Drafting Team	Response to comments: • RF: Footnote 1 page 1 added space after “references.” • RF: Changed “Tasf” to “Task” in Revision History. • Response to SERC CIPC and Southern Company comments to Draft 1. • Modified Question 1 to include reference to CIP-002. • Added an item to the R1 Compliance Assessment Approach to verify the effectiveness of the process. • Modified the R2 Compliance Assessment Approaches to clarify that the review is for implementation.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Reliability Standard Audit Worksheet[1]

CIP-012-1 – Cyber Security – Communications between Control Centers~~Control Center Communication Networks~~

This section to be completed by the Compliance Enforcement Authority.

Audit ID:	Audit ID if available; or REG-NCRnnnnn-YYYYMMDD
Registered Entity:	Registered name of entity being audited
NCR Number:	NCRnnnnn
Compliance Enforcement Authority:	Region or NERC performing audit
Compliance Assessment Date(s)[2]:	Month DD, YYYY, to Month DD, YYYY
Compliance Monitoring Method:	[On-site Audit | Off-site Audit | Spot Check]
Names of Auditors:	Supplied by CEA

Applicability of Requirements

	BA	DP	GO	GOP	PA/PC	RC	RP	RSG	TO	TOP	TP	TSP
R1	X		X	X		X			X	X		
R2	X		X	X		X			X	X		

Legend:

Text with blue background:	Fixed text – do not edit
Text entry area with Green background:	Entity-supplied information
Text entry area with white background:	Auditor-supplied information

[1] NERC developed this Reliability Standard Audit Worksheet (RSAW) language in order to facilitate NERC's and the Regional Entities' assessment of a registered entity's compliance with this Reliability Standard. The NERC RSAW language is written to specific versions of each NERC Reliability Standard. Entities using this RSAW should choose the version of the RSAW applicable to the Reliability Standard being assessed. While the information included in this RSAW provides some of the methodology that NERC has elected to use to assess compliance with the requirements of the Reliability Standard, this document should not be treated as a substitute for the Reliability Standard or viewed as additional Reliability Standard requirements. In all cases, the Regional Entity should rely on the language contained in the Reliability Standard itself, and not on the language contained in this RSAW, to determine compliance with the Reliability Standard. NERC's Reliability Standards can be found on NERC's website. Additionally, NERC Reliability Standards are updated frequently, and this RSAW may not necessarily be updated with the same frequency. Therefore, it is imperative that entities treat this RSAW as a reference document only, and not as a substitute or replacement for the Reliability Standard. It is the responsibility of the registered entity to verify its compliance with the latest approved version of the Reliability Standards, by the applicable governmental authority, relevant to its registration status.

The RSAW may provide a non-exclusive list, for informational purposes only, of examples of the types of evidence a registered entity may produce or may be asked to produce to demonstrate compliance with the Reliability Standard. A registered entity's adherence to the examples contained within this RSAW does not necessarily constitute compliance with the applicable Reliability Standard, and NERC and the Regional Entity using this RSAW reserve the right to request additional evidence from the registered entity that is not included in this RSAW. This RSAW may include excerpts from FERC Orders and other regulatory references which are provided for ease of reference only, and this document does not necessarily include all applicable Order provisions. In the event of a discrepancy between FERC Orders, and the language included in this document, FERC Orders shall prevail.

[2] Compliance Assessment Date(s): The date(s) the actual compliance assessment (on-site audit, off-site spot check, etc.) occurs.

Findings

(This section to be completed by the Compliance Enforcement Authority)

Req.	Finding	Summary and Documentation	Functions Monitored
R1			
R2			

Req.	Areas of Concern

Req.	Recommendations

Req.	Positive Observations

Subject Matter Experts

Identify the Subject Matter Expert(s) responsible for this Reliability Standard.

Registered Entity Response (Required; Insert additional rows if needed):

SME Name	Title	Organization	Requirement(s)

Registered Entity Response (Required):

Question 1[A1][A2]**:** Does the Registered Entity own or operate a Control Center? ☐ Yes ☐ No

If no:

1. Provide evidence in the space that the Registered Entity does not own or operate one or more Control Centers. This evidence may include, but is not limited to:
   - Evidence that the Registered Entity does not own or operate a Control Center; or
   - Evidence or a reference to evidence from the Registered Entity's CIP-002 compliance program that demonstrates the entity does not own or operate a Control Center.
   - ~~Evidence that the Registered Entity's asset list does not contain a Control Center.~~
2. The remainder of this RSAW may be left blank.

~~If yes, continue with Question 2.~~

[Note: A separate spreadsheet or other document may be used. If so, provide the document reference below.]

~~**Question 2:** Is data used for Operational Planning Analysis, Real-time Assessments, or Real-time monitoring and control transmitted between Control Centers at any time by any Control Center owned or operated by the Registered Entity? ☐ Yes ☐ No~~

~~If no:~~

1. ~~Provide evidence in the space below supporting this assertion. This evidence may include, but is not limited to:~~
   - ~~Evidence demonstrating data used for Operational Planning Analysis, Real-time Assessments, and Real-time monitoring and control is not transmitted between Control Centers at any time by any Control Center owned or operated by the Registered Entity.~~
2. ~~The remainder of this RSAW may be left blank.~~

~~If yes, continue with the remainder of this RSAW.~~

~~[Note: A separate spreadsheet or other document may be used. If so, provide the document reference below.]~~

R1 Supporting Evidence and Documentation

R1. The Responsible Entity shall develop one or more documented plan(s) to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring and control data while being transmitted between any Control Centers. This requirement excludes oral communications. The plan shall include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1 Identification of security protection used to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring and control data while being transmitted between Control Centers;

1.2 Identification of demarcation point(s) where security protection is applied for transmitting Real-time Assessment and Real-time monitoring and control data between Control Centers; and

1.3 Identification of roles and responsibilities of each Responsible Entity for applying security protection to the transmission of Real-time Assessment and Real-time monitoring and control data between Control Centers, when the Control Centers are owned or operated by different Responsible Entities.

~~The Responsible Entity shall develop one or more documented plan(s) to mitigate the risk of the unauthorized disclosure or modification of data used for Operational Planning Analysis, Real-time Assessments, and Real-time monitoring while being transmitted between Control Centers. This excludes oral communications. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*~~

~~**1.1** Risk mitigation shall be accomplished by one or more of the following actions:~~

- ~~Physically protecting the communication links transmitting the data;~~
- ~~Logically protecting the data during transmission; or~~
- ~~Using an equally effective method to mitigate the risk of unauthorized disclosure or modification of the data.~~

~~Note: If the Responsible Entity does not have a Control Center or it does not transmit the type of data specified in Requirement R1 of CIP-012-1 between two Control Centers, the requirements in CIP-012-1 would not apply to that entity.~~

M1. Evidence may include, but is not limited to, documented plan(s) that meet the security objective of Requirement R1.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-012-1, R1

This section to be completed by the Compliance Enforcement Authority

	If the Registered Entity has answered "No" to ~~either~~ Question 1 ~~or Question 2~~, verify~~:~~ ~~The~~the Registered Entity does not own or operate a Control Center. Note: If the Registered Entity does not own or operate a Control Center, the remainder of this RSAW is not applicable.~~; or~~ ~~The Registered Entity does not transmit data used for Operational Planning Analysis, Real-time Assessments, or Real-time monitoring and control at any time between Control Centers.~~
	Verify the entity has developed one or more documented plan(s) to mitigate the risk of the unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring and control data while being transmitted between Control Centers.
	Verify the documented plans collectively include identification of security protection used to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring and control data while being transmitted between Control Centers.
	Verify the documented plans collectively include identification of demarcation point(s) where security protection is applied for transmitting Real-time Assessment and Real-time monitoring and control data between Control Centers.~~; and~~
	~~If the Registered Entity has answered "Yes" to Question 2, verify:~~ ~~The entity has developed one or more documented plans to mitigate the risk of the unauthorized disclosure or modification of data used for Operational Planning Analysis, Real-time Assessments, and Real-time monitoring and control data while being transmitted between Control Centers; and~~ ~~The documented plans collectively include identification of security protection used to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring and control data while being transmitted between Control Centers; and~~ ~~The documented plans collectively include identification of demarcation point(s) where security protection is applied for transmitting Real-time Assessment and Real-time monitoring and control data between Control Centers; and~~ Verify the ~~The~~ documented plans collectively include identification of roles and responsibilities of each Responsible Entity for applying security protection to the transmission of Real-time Assessment and Real-time monitoring and control data between Control Centers, when the Control Centers are owned or operated by different Responsible Entities. ~~The documented plan(s) collectively address all data used for Operational Planning Analysis, Real-time Assessments, and Real-time monitoring transmitted between Control Centers; and~~ ~~The documented plan(s) collectively accomplish risk mitigation by one or more of the following actions:~~ ~~Physically protecting the communication links transmitting the data;~~ ~~Logically protecting the data during transmission; or~~ ~~Using an equally effective method to mitigate the risk of unauthorized disclosure or modification of the data.~~
	Verify the documented plans collectively achieve the security objective of mitigating the risk of the unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring and control data while being transmitted between Control Centers.
Note to Auditor: 1. Oral communications are not in scope for CIP-012-1.	

Auditor Notes:

R2 Supporting Evidence and Documentation

R2. The Responsible Entity shall implement the plan(s) specified in Requirement R1, except under CIP Exceptional Circumstances.

M2. Evidence may include, but is not limited to, documentation to demonstrate implementation of methods to mitigate the risk of the unauthorized disclosure or modification of data in Requirement R1.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-012-1, R2

This section to be completed by the Compliance Enforcement Authority

	~~If the Registered Entity has answered "Yes" to Question 2, verify with system-generated evidence (where available) that the Registered Entity has implemented the plan(s) specified in Requirement R1, except under CIP Exceptional Circumstances.~~
	Verify the entity has implemented one or more documented plan(s) to mitigate the risk of the unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring and control data while being transmitted between Control Centers.
	Verify the entity has identified security protection used to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring and control data while being transmitted between Control Centers.
	Verify the entity has identified demarcation point(s) where security protection is applied for transmitting Real-time Assessment and Real-time monitoring and control data between Control Centers;

	and
	Verify the entity has identified roles and responsibilities of each Responsible Entity for applying security protection to the transmission of Real-time Assessment and Real-time monitoring and control data between Control Centers, when the Control Centers are owned or operated by different Responsible Entities.
	If the Responsible Entity has declared and responded to CIP Exceptional Circumstances, verify the Responsible Entity has adhered to the applicable cyber security policies.
Note to Auditor: The Responsible Entity may reference a separate set of documents to demonstrate its response to any requirements impacted by CIP Exceptional Circumstances.	

Auditor Notes:

Additional Information:

Reliability Standard

The full text of CIP-012-1 may be found on the NERC Web Site (www.nerc.com) under "Program Areas & Departments", "Standards," "Reliability Standards."

In addition to the Reliability Standard, there is an applicable Implementation Plan available on the NERC Web Site.

In addition to the Reliability Standard, there is background information available on the NERC Web Site.

Capitalized terms in the Reliability Standard refer to terms in the NERC Glossary, which may be found on the NERC Web Site.

Sampling Methodology

Sampling is essential for auditing compliance with NERC Reliability Standards since it is not always possible or practical to test 100% of either the equipment, documentation, or both, associated with the full suite of enforceable standards. The Sampling Methodology Guidelines and Criteria (see NERC website), or sample guidelines, provided by the Electric Reliability Organization help to establish a minimum sample set for monitoring and enforcement uses in audits of NERC Reliability Standards.

Regulatory Language

FERC Order 822 P53-56, 58, and 62

Selected Glossary Terms

The following Glossary terms are provided for convenience only. Please refer to the NERC web site for the current enforceable terms.

CIP Exceptional Circumstance

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.

Control Center

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, of: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for transmission Facilities at two or more locations, or 4) a Generator Operator for generation Facilities at two or more locations.

~~Operational Planning Analysis~~

~~An evaluation of projected system conditions to assess anticipated (pre-Contingency) and potential (post-Contingency) conditions for next-day operations. The evaluation shall reflect applicable inputs including, but~~

~~not limited to, load forecasts; generation output levels; Interchange; known Protection System and Special Protection System status or degradation; Transmission outages; generator outages; Facility Ratings; and identified phase angle and equipment limitations. (Operational Planning Analysis may be provided through internal systems or through third-party services.)~~

Real-time Assessment

An evaluation of system conditions using Real-time data to assess existing (pre-Contingency) and potential (post-Contingency) operating conditions. The assessment shall reflect applicable inputs including, but not limited to: load, generation output levels, known Protection System and Special Protection System status or degradation, Transmission outages, generator outages, Interchange, Facility Ratings, and identified phase angle and equipment limitations. (Real-time Assessment may be provided through internal systems or through third-party services.)

Real-time

Present time as opposed to future time.

Revision History for RSAW

Version	Date	Reviewers	Revision Description
Draft1 v1	07/28/2017	NERC Stds Group	New document
Draft1 v2	08/01/2017	RSAW Task Force	Modified Question to clarify applicability
Draft1 v3	08/02/2017	RSAW Task Force	Response to MRO comments. Moved Questions 1 and 2 above R1. Made text changes to Q1 and to R2 Compliance Assessment Approach.
Draft1 v4	08/07/2017	RSAW Tas~~f~~k Force, 2016-02 SDT	Response to TexasRE and SDT comments. Clarified scope of Q1 to be data transmitted between Control Centers. Removed extra space from Auditor Notes.
Draft2 v1	10/27/2017	RSAW Task Force	Modified title. Modified Q2 to conform with new language. Modified R1 with new Requirement text and new Compliance Assessment Approach. Modified R2 with new Compliance Assessment Approach. Removed Operational Planning Analysis from the Selected Glossary Terms. Modified footer with revised version and date.
Draft2 v2	11/27/2017	RSAW Task Force	Response to comments: • RF: Footnote 1 page 1 added space after "references." • RF: Changed "Tasf" to "Task" in Revision History • Response to SERC CIPC and Southern Company comments to Draft 1. • Modified Question 1 to include reference to CIP-002. • Added an item to the R1 Compliance Assessment Approach to verify the effectiveness of the process. • Modified the R2 Compliance Assessment Approaches to clarify that the review is for implementation.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Reminder

Project 2016-02 Modifications to CIP Standards

Additional Ballot and Non-binding Poll Open through December 11, 2017

Now Available

An additional ballot for **CIP-012-1 – Cyber Security – Communications between Control Centers** and non-binding poll of the associated Violation Risk Factors and Violation Severity Levels are open through **8 p.m. Eastern, Monday, December 11, 2017.**

The standard drafting team's consideration of the responses received from the last comment period are reflected in this draft of the standard.

Balloting

Members of the ballot pools associated with this project can log in and submit their votes by accessing the Standards Balloting and Commenting System (SBS) here. If you experience any difficulties navigating the SBS, contact Wendy Muller.

- *If you are having difficulty accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out, contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern).*
- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*
- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Note: If a member cast a vote in the previous ballot, that vote will not carry over to this additional ballot. It is the responsibility of the registered voter in the ballot pool to cast a vote again in this ballot. To ensure a quorum is reached, if you do not want to vote affirmative or negative, cast an abstention.

Next Steps

The ballot results will be announced and posted on the project page. The drafting team will review all responses received during the comment period and determine the next steps of the project.

For information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact Katherine Street at (404) 446-9702 or Mat Bunch at (404) 446-9785.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2016-02 Modifications to CIP Standards

Formal Comment Period Open through December 11, 2017

Now Available

A 45-day formal comment period for **CIP-012-1 - Cyber Security – Communications between Control Centers** is open through **8 p.m. Eastern, Monday, December 11, 2017.**

The standard drafting team's considerations of the responses received from the last comment period are reflected in this draft of the standard.

Commenting

Use the Standards Balloting and Commenting System (SBS) to submit comments. If you experience issues navigating the SBS, contact Wendy Muller. An unofficial Word version of the comment form is posted on the project page.

- *If you are having difficulty accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out, contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern).*
- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*
- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Next Steps

An additional ballot for the standard and non-binding poll of the associated Violation Risk Factors and Violation Severity Levels will be conducted **December 1-11, 2017**.

For information on the Standards Development Process, refer to the Standard Processes Manual**.**

For more information or assistance, contact Katherine Street at (404) 446-9702 or Mat Bunch at (404) 446-9785.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/113)
Ballot Name: 2016-02 Modifications to CIP Standards CIP-012-1 AB 2 ST
Voting Start Date: 12/1/2017 12:01:00 AM
Voting End Date: 12/11/2017 8:00:00 PM
Ballot Type: ST
Ballot Activity: AB
Ballot Series: 2
Total # Votes: 239
Total Ballot Pool: 309
Quorum: 77.35
Weighted Segment Value: 63.91

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	80	1	30	0.556	24	0.444	3	7	16
Segment: 2	7	0.5	4	0.4	1	0.1	0	0	2
Segment: 3	73	1	31	0.596	21	0.404	1	3	17
Segment: 4	17	1	7	0.583	5	0.417	0	0	5
Segment: 5	73	1	24	0.5	24	0.5	1	3	21
Segment: 6	46	1	21	0.583	15	0.417	1	1	8
Segment: 7	2	0.1	1	0.1	0	0	0	0	1
Segment: 8	3	0.3	3	0.3	0	0	0	0	0
Segment: 9	1	0.1	1	0.1	0	0	0	0	0
Segment: 10	7	0.6	5	0.5	1	0.1	0	1	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Totals:	309	6.6	127	4.218	91	2.382	6	15	70

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Negative	Comments Submitted
1	Allete - Minnesota Power, Inc.	Jamie Monette		Abstain	N/A
1	American Transmission Company, LLC	Douglas Johnson		Negative	No Comment Submitted
1	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	John Shaver		None	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		None	N/A
1	Balancing Authority of Northern California	Kevin Smith	Joe Tarantino	Negative	Comments Submitted
1	Basin Electric Power Cooperative	David Rudolph		None	N/A
1	BC Hydro and Power Authority	Patricia Robertson		None	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Bonneville Power Administration	Kammy Rogers-Holliday		Negative	Comments Submitted
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		Negative	No Comment Submitted
1	Cedar Falls Utilities	Adam Peterson		None	N/A
1	CenterPoint Energy Houston Electric, LLC	John Brockhan		Negative	Comments Submitted
1	Central Electric Power Cooperative (Missouri)	Michael Bax		None	N/A
1	Central Hudson Gas & Electric Corp.	Frank Pace		Affirmative	N/A
1	City Utilities of Springfield, Missouri	Michael Buyce		Affirmative	N/A
1	CMS Energy - Consumers Energy Company	James Anderson		None	N/A
1	Con Ed - Consolidated Edison Co. of New York	Daniel Grinkevich		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Larry Nash		Negative	Comments Submitted
1	Duke Energy	Laura Lee		Affirmative	N/A
1	Edison International - Southern California Edison Company	Steven Mavis		Affirmative	N/A
1	Entergy - Entergy Services, Inc.	Oliver Burke		Abstain	N/A
1	Eversource Energy	Quintin Lee		None	N/A
1	Exelon	Chris Scanlon		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	Karen Yoder		Affirmative	N/A
1	Great Plains Energy - Kansas City Power and Light Co.	James McBee	Douglas Webb	Affirmative	N/A
1	Great River Energy	Gordon Pietsch		None	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Oshani Pathirane	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Affirmative	N/A
1	IDACORP - Idaho Power Company	Laura Nelson		Abstain	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz		Abstain	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Stephanie Burns	Negative	Third-Party Comments
1	Lincoln Electric System	Danny Pudenz		Negative	Third-Party Comments
1	Long Island Power Authority	Robert Ganley		Affirmative	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	Michael Shaw		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Mike Smith		Affirmative	N/A
1	MEAG Power	David Weekley	Scott Miller	Abstain	N/A
1	Memphis Light, Gas and Water Division	Allan Long		None	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard		Negative	Third-Party Comments
1	Muscatine Power and Water	Andy Kurriger		Negative	Third-Party Comments
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Negative	Third-Party Comments
1	Nebraska Public Power District	Jamison Cawley		Negative	Third-Party Comments
1	New York Power Authority	Salvatore Spagnolo		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		None	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Affirmative	N/A
1	Northeast Missouri Electric Power Cooperative	Kevin White		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Abstain	N/A
1	Ohio Valley Electric Corporation	Scott Cunningham		Negative	Third-Party Comments
1	Omaha Public Power District	Doug Peterchuck		None	N/A
1	Oncor Electric Delivery	Lee Maurer	Tho Tran	Abstain	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		Negative	Third-Party Comments
1	Peak Reliability	Scott Downey		Affirmative	N/A
1	PNM Resources - Public Service Company of New Mexico	Laurie Williams		Affirmative	N/A
1	PPL Electric Utilities Corporation	Brenda Truhe		Affirmative	N/A
1	PSEG - Public Service Electric and Gas Co.	Joseph Smith		Affirmative	N/A
1	Public Utility District No. 1 of Chelan County	Jeff Kimbell		Negative	Comments Submitted
1	Public Utility District No. 1 of Snohomish County	Long Duong		Negative	Third-Party Comments
1	Puget Sound Energy, Inc.	Theresa Rakowsky		Affirmative	N/A
1	Sacramento Municipal Utility District	Arthur Starkovich	Joe Tarantino	Negative	Comments Submitted
1	Salt River Project	Steven Cobb		None	N/A
1	Santee Cooper	Shawn Abrams		Negative	No Comment Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	SCANA - South Carolina Electric and Gas Co.	Tom Hanzlik		None	N/A
1	Seattle City Light	Pawel Krupa		Negative	Third-Party Comments
1	Seminole Electric Cooperative, Inc.	Mark Churilla		Negative	Comments Submitted
1	Sempra - San Diego Gas and Electric	Martine Blair	Jeff Johnson	Negative	Third-Party Comments
1	Sho-Me Power Electric Cooperative	Peter Dawson		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Katherine Prewitt		Affirmative	N/A
1	Southern Indiana Gas and Electric Co.	Steve Rawlinson		Affirmative	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell		Negative	Comments Submitted
1	Tennessee Valley Authority	Howell Scott		Affirmative	N/A
1	Tri-State G and T Association, Inc.	Tracy Sliman		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Negative	Comments Submitted
1	Westar Energy	Kevin Giles		Affirmative	N/A
1	Western Area Power Administration	sean erickson		Negative	Comments Submitted
1	Xcel Energy, Inc.	Dean Schiro		None	N/A
2	California ISO	Richard Vine		Affirmative	N/A
2	Electric Reliability Council of Texas, Inc.	Elizabeth Axson		Affirmative	N/A
2	Independent Electricity System Operator	Leonard Kula		Affirmative	N/A
2	ISO New England, Inc.	Michael Puscas		None	N/A
2	Midcontinent ISO, Inc.	Ellen Oswald		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
2	New York Independent System Operator	Gregory Campoli		None	N/A
2	PJM Interconnection, L.L.C.	Mark Holman		Affirmative	N/A
3	AEP	Aaron Austin		Negative	Comments Submitted
3	AES - Indianapolis Power and Light Co.	Bette White		None	N/A
3	APS - Arizona Public Service Co.	Vivian Vo		Affirmative	N/A
3	Arkansas Electric Cooperative Corporation	Mark Gann		None	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	W. Dwayne Preston		Negative	Comments Submitted
3	Basin Electric Power Cooperative	Jeremy Voll		Affirmative	N/A
3	BC Hydro and Power Authority	Hootan Jarollahi		None	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Annette Johnston		Negative	Comments Submitted
3	Bonneville Power Administration	Rebecca Berdahl		Negative	Comments Submitted
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City of Farmington	Linda Jacobson-Quinn		None	N/A
3	City of Leesburg	Chris Adkins		Affirmative	N/A
3	City of Vero Beach	Ginny Beigel	Brandon McCormick	Affirmative	N/A
3	City Utilities of Springfield, Missouri	Scott Williams		Affirmative	N/A
3	Cleco Corporation	Michelle Corley	Louis Guidry	Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
3	Cowlitz County PUD	Russell Noble		None	N/A
3	Duke Energy	Lee Schuster		Affirmative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		None	N/A
3	Empire District Electric Co.	Kalem Long		None	N/A
3	Eversource Energy	Sharon Flannery		None	N/A
3	Exelon	John Bee		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		None	N/A
3	Great Plains Energy - Kansas City Power and Light Co.	Jessica Tucker	Douglas Webb	Affirmative	N/A
3	Great River Energy	Brian Glover		Negative	Third-Party Comments
3	Hydro One Networks, Inc.	Paul Malozewski		None	N/A
3	KAMO Electric Cooperative	Ted Hilmes		None	N/A
3	Lincoln Electric System	Jason Fortik		Negative	Third-Party Comments
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	Manitoba Hydro	Karim Abdel-Hadi		Affirmative	N/A
3	MEAG Power	Roger Brand	Scott Miller	Abstain	N/A
3	Modesto Irrigation District	Jack Savage	Nick Braden	Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Negative	Third-Party Comments
3	National Grid USA	Brian Shanahan		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Nebraska Public Power District	Tony Eddleman		Negative	Third-Party Comments
3	New York Power Authority	David Rivera		Affirmative	N/A
3	NiSource - Northern Indiana Public Service Co.	Aimee Harris		Affirmative	N/A
3	North Carolina Electric Membership Corporation	doug white	Scott Brame	Affirmative	N/A
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		None	N/A
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen		None	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Abstain	N/A
3	OTP - Otter Tail Power Company	Wendi Olson		Negative	Third-Party Comments
3	Owensboro Municipal Utilities	Thomas Lyons		Affirmative	N/A
3	Platte River Power Authority	Jeff Landis		Negative	Third-Party Comments
3	PNM Resources - Public Service Company of New Mexico	Lynn Goldstein		Affirmative	N/A
3	Portland General Electric Co.	Angela Gaines		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	Charles Freibert		Affirmative	N/A
3	PSEG - Public Service Electric and Gas Co.	Jeffrey Mueller		Affirmative	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Negative	Comments Submitted
3	Puget Sound Energy, Inc.	Lynda Kupfer		Affirmative	N/A
3	Rutherford EMC	Tom Haire		Abstain	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Joe Tarantino	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Salt River Project	Rudy Navarro		Negative	Comments Submitted
3	Santee Cooper	James Poston		Negative	No Comment Submitted
3	SCANA - South Carolina Electric and Gas Co.	Scott Parker		None	N/A
3	Seattle City Light	Tuan Tran		Negative	Third-Party Comments
3	Seminole Electric Cooperative, Inc.	James Frauen		Negative	Comments Submitted
3	Sempra - San Diego Gas and Electric	Bridget Silvia	Harold Sherrill	Negative	Third-Party Comments
3	Sho-Me Power Electric Cooperative	Jeff Neas		Affirmative	N/A
3	Silicon Valley Power - City of Santa Clara	Val Ridad		None	N/A
3	Snohomish County PUD No. 1	Mark Oens		Negative	Third-Party Comments
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Fred Frederick		None	N/A
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson		Negative	Comments Submitted
3	TECO - Tampa Electric Co.	Ronald Donahey		Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A
3	Tri-State G and T Association, Inc.	Janelle Marriott Gill		None	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Affirmative	N/A
3	Westar Energy	Bo Jones		Affirmative	N/A
3	Xcel Energy, Inc.	Michael Ibold		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	American Public Power Association	Jack Cashin		None	N/A
4	Arkansas Electric Cooperative Corporation	Alice Wright		None	N/A
4	Austin Energy	Esther Weekes		Negative	Comments Submitted
4	City of Clewiston	Lynne Mila	Brandon McCormick	Affirmative	N/A
4	City Utilities of Springfield, Missouri	John Allen		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Aubrey Short		Affirmative	N/A
4	Georgia System Operations Corporation	Guy Andrews		Affirmative	N/A
4	Indiana Municipal Power Agency	Jack Alvey	Scott Berry	None	N/A
4	National Rural Electric Cooperative Association	Barry Lawson		Affirmative	N/A
4	North Carolina Electric Membership Corporation	John Lemire	Scott Brame	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John Martinsen		Negative	Third-Party Comments
4	Sacramento Municipal Utility District	Beth Tincher	Joe Tarantino	Negative	Comments Submitted
4	Seattle City Light	Hao Li		Negative	Third-Party Comments
4	Seminole Electric Cooperative, Inc.	Charles Wubbena		Negative	Comments Submitted
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Shirley Eshbach	None	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		None	N/A
4	WEC Energy Group, Inc.	Anthony Jankowski		Affirmative	N/A
5	Acciona Energy North America	George Brown		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	AEP	Thomas Foltz		Negative	Comments Submitted
5	Ameren - Ameren Missouri	Sam Dwyer		Abstain	N/A
5	APS - Arizona Public Service Co.	Linda Henrickson		Affirmative	N/A
5	Arkansas Electric Cooperative Corporation	Moses Harris		None	N/A
5	Associated Electric Cooperative, Inc.	Brad Haralson		Affirmative	N/A
5	Austin Energy	Jeanie Doty		Negative	Comments Submitted
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	Basin Electric Power Cooperative	Mike Kraft		None	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		None	N/A
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		Negative	Third-Party Comments
5	Bonneville Power Administration	Francis Halpin		Negative	Comments Submitted
5	BP Wind Energy North America Inc.	Carla Holly		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
5	Cleco Corporation	Stephanie Huffman	Louis Guidry	Negative	Third-Party Comments
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Negative	Comments Submitted
5	Colorado Springs Utilities	Jeff Icke		Negative	Comments Submitted
5	Con Ed - Consolidated Edison Co. of New York	William Winters	Alyson Slanover	Affirmative	N/A
5	Dairyland Power Cooperative	Tommy Drea		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Dominion - Dominion Resources, Inc.	Lou Oberski		Negative	Comments Submitted
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	Edison International - Southern California Edison Company	Selene Willis		None	N/A
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy	Jamie Prater		Affirmative	N/A
5	Exelon	Ruth Miller		Affirmative	N/A
5	FirstEnergy - FirstEnergy Solutions	Robert Loy		Affirmative	N/A
5	Great Plains Energy - Kansas City Power and Light Co.	Harold Wyble	Douglas Webb	Affirmative	N/A
5	Great River Energy	Preston Walsh		Negative	Third-Party Comments
5	Gridforce Energy Management, LLC	David Blackshear		None	N/A
5	Hydro-Qu?bec Production	Junji Yamaguchi		None	N/A
5	JEA	John Babik		None	N/A
5	Kissimmee Utility Authority	Mike Blough		Affirmative	N/A
5	Lakeland Electric	Jim Howard		None	N/A
5	Lincoln Electric System	Kayleigh Wilkerson		Negative	Third-Party Comments
5	Los Angeles Department of Water and Power	Glenn Barry		None	N/A
5	Manitoba Hydro	Yuguang Xiao		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	David Gordon		Affirmative	N/A
5	MEAG Power	Steven Grego	Scott Miller	Abstain	N/A
5	Muscatine Power and Water	Neal Nelson		None	N/A
5	NB Power Corporation	Laura McLeod		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Nebraska Public Power District	Don Schmit		Negative	Third-Party Comments
5	New York Power Authority	Randy Crissman		Affirmative	N/A
5	NextEra Energy	Allen Schriver		None	N/A
5	NiSource - Northern Indiana Public Service Co.	Dmitriy Bazylyuk		Affirmative	N/A
5	North Carolina Electric Membership Corporation	Robert Beadle	Scott Brame	Affirmative	N/A
5	Northern California Power Agency	Marty Hostler		None	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	John Rhea		None	N/A
5	Omaha Public Power District	Mahmood Safi		Negative	Third-Party Comments
5	Ontario Power Generation Inc.	David Ramkalawan		Affirmative	N/A
5	OTP - Otter Tail Power Company	Cathy Fogale		Negative	Third-Party Comments
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	Dan Wilson		Affirmative	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Affirmative	N/A
5	Public Utility District No. 1 of Chelan County	Haley Sousa		Negative	Comments Submitted
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Negative	Third-Party Comments
5	Puget Sound Energy, Inc.	Eleanor Ewry		Affirmative	N/A
5	Sacramento Municipal Utility District	Susan Oto	Joe Tarantino	Negative	Comments Submitted
5	Salt River Project	Kevin Nielsen		Negative	Comments Submitted
5	Santee Cooper	Tommy Curtis		Negative	No Comment Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	SCANA - South Carolina Electric and Gas Co.	Alyssa Hubbard		None	N/A
5	Seattle City Light	Mike Haynes		Negative	Third-Party Comments
5	Seminole Electric Cooperative, Inc.	Brenda Atkins		None	N/A
5	Sempra - San Diego Gas and Electric	Jerome Gobby	Andrey Komissarov	Negative	Third-Party Comments
5	Silicon Valley Power - City of Santa Clara	Sandra Pacheco		None	N/A
5	Southern Company - Southern Company Generation	William D. Shultz		Affirmative	N/A
5	SunPower	Bradley Collard		None	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin		Negative	Comments Submitted
5	Talen Generation, LLC	Donald Lock		Negative	Comments Submitted
5	TECO - Tampa Electric Co.	R James Rocha		Affirmative	N/A
5	Tennessee Valley Authority	M Lee Thomas		Affirmative	N/A
5	U.S. Bureau of Reclamation	Wendy Center		Negative	Comments Submitted
5	WEC Energy Group, Inc.	Linda Horn		Affirmative	N/A
5	Xcel Energy, Inc.	Gerry Huitt		Negative	Comments Submitted
6	APS - Arizona Public Service Co.	Jonathan Aragon		Affirmative	N/A
6	Arkansas Electric Cooperative Corporation	Bruce Walkup		None	N/A
6	Austin Energy	Andrew Gallo		Negative	Comments Submitted
6	Basin Electric Power Cooperative	Paul Huettl		Affirmative	N/A
6	Berkshire Hathaway - PacifiCorp	Sandra Shaffer		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Bonneville Power Administration	Andrew Meyers		Negative	Comments Submitted
6	Cleco Corporation	Robert Hirchak	Louis Guidry	Negative	Third-Party Comments
6	Con Ed - Consolidated Edison Co. of New York	Robert Winston		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
6	Duke Energy	Greg Cecil		Affirmative	N/A
6	Edison International - Southern California Edison Company	Kenya Streeter		None	N/A
6	Entergy	Julie Hall		Affirmative	N/A
6	Exelon	Becky Webb		Affirmative	N/A
6	FirstEnergy - FirstEnergy Solutions	Ann Ivanc		Affirmative	N/A
6	Florida Municipal Power Pool	Tom Reedy	Brandon McCormick	Affirmative	N/A
6	Great Plains Energy - Kansas City Power and Light Co.	Jim Flucke	Douglas Webb	Affirmative	N/A
6	Lincoln Electric System	Eric Ruskamp		Negative	Third-Party Comments
6	Los Angeles Department of Water and Power	Anton Vu		Affirmative	N/A
6	Luminant - Luminant Energy	Brenda Hampton		Affirmative	N/A
6	Manitoba Hydro	Blair Mukanik		Affirmative	N/A
6	Modesto Irrigation District	James McFall	Nick Braden	Affirmative	N/A
6	Muscatine Power and Water	Ryan Streck		Negative	Third-Party Comments
6	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		None	N/A
6	NiSource - Northern Indiana Public Service Co.	Joe O'Brien		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Northern California Power Agency	Dennis Sismaet		None	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay		None	N/A
6	Omaha Public Power District	Joel Robles		None	N/A
6	Portland General Electric Co.	Daniel Mason		Affirmative	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
6	Public Utility District No. 1 of Chelan County	Janis Weddle		Negative	Comments Submitted
6	Public Utility District No. 2 of Grant County, Washington	LeRoy Patterson		None	N/A
6	Sacramento Municipal Utility District	Jamie Cutlip	Joe Tarantino	Negative	Comments Submitted
6	Salt River Project	Bobby Olsen		Negative	Comments Submitted
6	Santee Cooper	Michael Brown		Negative	No Comment Submitted
6	Seattle City Light	Charles Freeman		Negative	Third-Party Comments
6	Seminole Electric Cooperative, Inc.	Trudy Novak		Negative	Comments Submitted
6	Snohomish County PUD No. 1	Franklin Lu		Negative	Third-Party Comments
6	Southern Company - Southern Company Generation and Energy Marketing	Jennifer Sykes		Affirmative	N/A
6	Southern Indiana Gas and Electric Co.	Brad Lisembee		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Rick Applegate		Negative	Comments Submitted
6	Talen Energy Marketing, LLC	Jennifer Hohenshilt		Negative	Comments Submitted
6	TECO - Tampa Electric Co.	Benjamin Smith		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Tennessee Valley Authority	Marjorie Parsons		Affirmative	N/A
6	WEC Energy Group, Inc.	Scott Hoggatt		Affirmative	N/A
6	Westar Energy	Megan Wagner		Affirmative	N/A
6	Xcel Energy, Inc.	Carrie Dixon		Negative	Comments Submitted
7	Exxon Mobil	Jay Barnett		None	N/A
7	Luminant Mining Company LLC	Stewart Rake		Affirmative	N/A
8	David Kiguel	David Kiguel		Affirmative	N/A
8	Massachusetts Attorney General	Frederick Plett		Affirmative	N/A
8	Roger Zaklukiewicz	Roger Zaklukiewicz		Affirmative	N/A
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson		Affirmative	N/A
10	Midwest Reliability Organization	Russel Mountjoy		Abstain	N/A
10	New York State Reliability Council	ALAN ADAMSON		Affirmative	N/A
10	Northeast Power Coordinating Council	Guy V. Zito		Affirmative	N/A
10	ReliabilityFirst	Anthony Jablonski		Affirmative	N/A
10	SERC Reliability Corporation	Drew Slabaugh		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Negative	Comments Submitted
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 309 of 309 entries

BALLOT RESULTS

Ballot Name: 2016-02 Modifications to CIP Standards CIP-012-1 Non-binding Poll AB 2 NB
Voting Start Date: 12/1/2017 12:01:00 AM
Voting End Date: 12/12/2017 8:00:00 PM
Ballot Type: NB
Ballot Activity: AB
Ballot Series: 2
Total # Votes: 228
Total Ballot Pool: 290
Quorum: 78.62
Weighted Segment Value: 60.44

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 1	75	1	28	0.56	22	0.44	15	10
Segment: 2	7	0.5	4	0.4	1	0.1	0	2
Segment: 3	70	1	27	0.614	17	0.386	12	14
Segment: 4	14	0.9	6	0.6	3	0.3	0	5
Segment: 5	69	1	19	0.5	19	0.5	11	20
Segment: 6	42	1	17	0.63	10	0.37	5	10
Segment: 7	2	0.1	1	0.1	0	0	0	1
Segment: 8	3	0.3	3	0.3	0	0	0	0
Segment: 9	1	0.1	1	0.1	0	0	0	0
Segment: 10	7	0.4	4	0.4	0	0	3	0
Totals:	290	6.3	110	4.203	72	2.097	46	62

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Negative	Comments Submitted
1	American Transmission Company, LLC	Douglas Johnson		Negative	Comments Submitted
1	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	John Shaver		None	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		None	N/A
1	Balancing Authority of Northern California	Kevin Smith	Joe Tarantino	Negative	Comments Submitted
1	Basin Electric Power Cooperative	David Rudolph		Affirmative	N/A
1	BC Hydro and Power Authority	Patricia Robertson		Abstain	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Negative	Comments Submitted
1	Bonneville Power Administration	Kammy Rogers-Holliday		Negative	Comments Submitted
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		Negative	Comments Submitted
1	Cedar Falls Utilities	Adam Peterson		None	N/A
1	CenterPoint Energy Houston Electric, LLC	John Brockhan		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Central Electric Power Cooperative (Missouri)	Michael Bax		None	N/A
1	Central Hudson Gas & Electric Corp.	Frank Pace		Affirmative	N/A
1	City Utilities of Springfield, Missouri	Michael Buyce		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Daniel Grinkevich		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Larry Nash		Abstain	N/A
1	Duke Energy	Laura Lee		Affirmative	N/A
1	Edison International - Southern California Edison Company	Steven Mavis		Affirmative	N/A
1	Entergy - Entergy Services, Inc.	Oliver Burke		Abstain	N/A
1	Eversource Energy	Quintin Lee		Affirmative	N/A
1	Exelon	Chris Scanlon		Abstain	N/A
1	FirstEnergy - FirstEnergy Corporation	Karen Yoder		Affirmative	N/A
1	Great Plains Energy - Kansas City Power and Light Co.	James McBee	Douglas Webb	Affirmative	N/A
1	Great River Energy	Gordon Pietsch		None	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Oshani Pathirane	Negative	Comments Submitted
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Affirmative	N/A
1	IDACORP - Idaho Power Company	Laura Nelson		Affirmative	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz		Abstain	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Stephanie Burns	Negative	Comments Submitted
1	Lincoln Electric System	Danny Pudenz		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Long Island Power Authority	Robert Ganley		Abstain	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	Michael Shaw		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Mike Smith		Affirmative	N/A
1	MEAG Power	David Weekley	Scott Miller	Abstain	N/A
1	Memphis Light, Gas and Water Division	Allan Long		Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard		Abstain	N/A
1	Muscatine Power and Water	Andy Kurriger		Negative	Comments Submitted
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Negative	Comments Submitted
1	Nebraska Public Power District	Jamison Cawley		Abstain	N/A
1	New York Power Authority	Salvatore Spagnolo		Affirmative	N/A
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		None	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Affirmative	N/A
1	Northeast Missouri Electric Power Cooperative	Kevin White		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Abstain	N/A
1	Ohio Valley Electric Corporation	Scott Cunningham		Negative	Comments Submitted
1	Omaha Public Power District	Doug Peterchuck		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	OTP - Otter Tail Power Company	Charles Wicklund		Negative	Comments Submitted
1	Peak Reliability	Scott Downey		None	N/A
1	PNM Resources - Public Service Company of New Mexico	Laurie Williams		Affirmative	N/A
1	PPL Electric Utilities Corporation	Brenda Truhe		Abstain	N/A
1	PSEG - Public Service Electric and Gas Co.	Joseph Smith		Abstain	N/A
1	Public Utility District No. 1 of Chelan County	Jeff Kimbell		None	N/A
1	Public Utility District No. 1 of Snohomish County	Long Duong		Negative	Comments Submitted
1	Puget Sound Energy, Inc.	Theresa Rakowsky		Affirmative	N/A
1	Sacramento Municipal Utility District	Arthur Starkovich	Joe Tarantino	Negative	Comments Submitted
1	Salt River Project	Steven Cobb		None	N/A
1	Santee Cooper	Shawn Abrams		Abstain	N/A
1	SCANA - South Carolina Electric and Gas Co.	Tom Hanzlik		Abstain	N/A
1	Seattle City Light	Pawel Krupa		Negative	Comments Submitted
1	Seminole Electric Cooperative, Inc.	Mark Churilla		Negative	Comments Submitted
1	Sempra - San Diego Gas and Electric	Martine Blair	Jeff Johnson	Negative	Comments Submitted
1	Sho-Me Power Electric Cooperative	Peter Dawson		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Katherine Prewitt		Affirmative	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Tennessee Valley Authority	Howell Scott		Affirmative	N/A
1	Tri-State G and T Association, Inc.	Tracy Sliman		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Negative	Comments Submitted
1	Westar Energy	Kevin Giles		Affirmative	N/A
1	Western Area Power Administration	sean erickson		Negative	Comments Submitted
2	California ISO	Richard Vine		Affirmative	N/A
2	Electric Reliability Council of Texas, Inc.	Elizabeth Axson		Affirmative	N/A
2	Independent Electricity System Operator	Leonard Kula		Affirmative	N/A
2	ISO New England, Inc.	Michael Puscas		None	N/A
2	Midcontinent ISO, Inc.	Ellen Oswald		Negative	Comments Submitted
2	New York Independent System Operator	Gregory Campoli		None	N/A
2	PJM Interconnection, L.L.C.	Mark Holman		Affirmative	N/A
3	AEP	Aaron Austin		Negative	Comments Submitted
3	AES - Indianapolis Power and Light Co.	Bette White		Affirmative	N/A
3	APS - Arizona Public Service Co.	Vivian Vo		Affirmative	N/A
3	Arkansas Electric Cooperative Corporation	Philip Huff		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	W. Dwayne Preston		Negative	Comments Submitted
3	Basin Electric Power Cooperative	Jeremy Voll		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Annette Johnston		Negative	Comments Submitted
3	Bonneville Power Administration	Rebecca Berdahl		Negative	Comments Submitted
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City of Farmington	Linda Jacobson-Quinn		None	N/A
3	City of Leesburg	Chris Adkins		Affirmative	N/A
3	City of Vero Beach	Ginny Beigel	Brandon McCormick	Affirmative	N/A
3	City Utilities of Springfield, Missouri	Scott Williams		Affirmative	N/A
3	Cleco Corporation	Michelle Corley	Louis Guidry	Abstain	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
3	Cowlitz County PUD	Russell Noble		None	N/A
3	Duke Energy	Lee Schuster		Affirmative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		None	N/A
3	Eversource Energy	Sharon Flannery		None	N/A
3	Exelon	John Bee		Abstain	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		None	N/A
3	Great Plains Energy - Kansas City Power and Light Co.	Jessica Tucker	Douglas Webb	Affirmative	N/A
3	Great River Energy	Brian Glover		Negative	Comments Submitted
3	Hydro One Networks, Inc.	Paul Malozewski		None	N/A
3	KAMO Electric Cooperative	Ted Hilmes		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Lincoln Electric System	Jason Fortik		Abstain	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	Manitoba Hydro	Karim Abdel-Hadi		Affirmative	N/A
3	MEAG Power	Roger Brand	Scott Miller	Abstain	N/A
3	Modesto Irrigation District	Jack Savage	Nick Braden	Abstain	N/A
3	Muscatine Power and Water	Seth Shoemaker		Negative	Comments Submitted
3	National Grid USA	Brian Shanahan		Negative	Comments Submitted
3	Nebraska Public Power District	Tony Eddleman		Abstain	N/A
3	New York Power Authority	David Rivera		Affirmative	N/A
3	NiSource - Northern Indiana Public Service Co.	Aimee Harris		Affirmative	N/A
3	North Carolina Electric Membership Corporation	doug white	Scott Brame	Affirmative	N/A
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		None	N/A
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen		None	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Abstain	N/A
3	OTP - Otter Tail Power Company	Wendi Olson		Negative	Comments Submitted
3	Owensboro Municipal Utilities	Thomas Lyons		Affirmative	N/A
3	Platte River Power Authority	Jeff Landis		Negative	Comments Submitted
3	PNM Resources - Public Service Company of New Mexico	Lynn Goldstein		Affirmative	N/A
3	Portland General Electric Co.	Angela Gaines		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	PPL - Louisville Gas and Electric Co.	Charles Freibert		None	N/A
3	PSEG - Public Service Electric and Gas Co.	Jeffrey Mueller		Abstain	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Negative	Comments Submitted
3	Puget Sound Energy, Inc.	Lynda Kupfer		Affirmative	N/A
3	Rutherford EMC	Tom Haire		Abstain	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Joe Tarantino	Negative	Comments Submitted
3	Salt River Project	Rudy Navarro		Negative	Comments Submitted
3	Santee Cooper	James Poston		Abstain	N/A
3	SCANA - South Carolina Electric and Gas Co.	Scott Parker		None	N/A
3	Seattle City Light	Tuan Tran		Negative	Comments Submitted
3	Seminole Electric Cooperative, Inc.	James Frauen		Negative	Comments Submitted
3	Sempra - San Diego Gas and Electric	Bridget Silvia	Harold Sherrill	Negative	Comments Submitted
3	Sho-Me Power Electric Cooperative	Jeff Neas		Affirmative	N/A
3	Silicon Valley Power - City of Santa Clara	Val Ridad		None	N/A
3	Snohomish County PUD No. 1	Mark Oens		Negative	Comments Submitted
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson		Negative	Comments Submitted
3	TECO - Tampa Electric Co.	Ronald Donahey		None	N/A
3	Tennessee Valley Authority	Ian Grant		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Tri-State G and T Association, Inc.	Janelle Marriott Gill		None	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Affirmative	N/A
3	Westar Energy	Bo Jones		Affirmative	N/A
3	Xcel Energy, Inc.	Michael Ibold		Abstain	N/A
4	American Public Power Association	Jack Cashin		None	N/A
4	Austin Energy	Esther Weekes		Affirmative	N/A
4	City of Clewiston	Lynne Mila	Brandon McCormick	Affirmative	N/A
4	City Utilities of Springfield, Missouri	John Allen		Affirmative	N/A
4	Georgia System Operations Corporation	Guy Andrews		Affirmative	N/A
4	Indiana Municipal Power Agency	Jack Alvey	Scott Berry	None	N/A
4	North Carolina Electric Membership Corporation	John Lemire	Scott Brame	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John Martinsen		Negative	Comments Submitted
4	Sacramento Municipal Utility District	Beth Tincher	Joe Tarantino	Negative	Comments Submitted
4	Seattle City Light	Hao Li		Negative	Comments Submitted
4	Seminole Electric Cooperative, Inc.	Charles Wubbena		None	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Shirley Eshbach	None	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		None	N/A
4	WEC Energy Group, Inc.	Anthony Jankowski		Affirmative	N/A
5	Acciona Energy North America	George Brown		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	AEP	Thomas Foltz		Negative	Comments Submitted
5	Ameren - Ameren Missouri	Sam Dwyer		Abstain	N/A
5	APS - Arizona Public Service Co.	Linda Henrickson		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Brad Haralson		Affirmative	N/A
5	Austin Energy	Jeanie Doty		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	Basin Electric Power Cooperative	Mike Kraft		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		None	N/A
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		Negative	Comments Submitted
5	Bonneville Power Administration	Francis Halpin		Negative	Comments Submitted
5	BP Wind Energy North America Inc.	Carla Holly		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
5	Cleco Corporation	Stephanie Huffman	Louis Guidry	Abstain	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Negative	Comments Submitted
5	Colorado Springs Utilities	Jeff Icke		Negative	Comments Submitted
5	Con Ed - Consolidated Edison Co. of New York	William Winters	Alyson Slanover	Affirmative	N/A
5	Dairyland Power Cooperative	Tommy Drea		Negative	Comments Submitted
5	Dominion - Dominion Resources, Inc.	Lou Oberski		Negative	Comments Submitted
5	Duke Energy	Dale Goodwine		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Edison International - Southern California Edison Company	Selene Willis		None	N/A
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy	Jamie Prater		Affirmative	N/A
5	Exelon	Ruth Miller		Abstain	N/A
5	FirstEnergy - FirstEnergy Solutions	Robert Loy		Affirmative	N/A
5	Great Plains Energy - Kansas City Power and Light Co.	Harold Wyble	Douglas Webb	Affirmative	N/A
5	Great River Energy	Preston Walsh		Negative	Comments Submitted
5	Hydro-Qu?bec Production	Junji Yamaguchi		None	N/A
5	JEA	John Babik		Negative	Comments Submitted
5	Kissimmee Utility Authority	Mike Blough		Affirmative	N/A
5	Lakeland Electric	Jim Howard		None	N/A
5	Lincoln Electric System	Kayleigh Wilkerson		Abstain	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		None	N/A
5	Manitoba Hydro	Yuguang Xiao		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	David Gordon		Abstain	N/A
5	MEAG Power	Steven Grego	Scott Miller	Abstain	N/A
5	Muscatine Power and Water	Neal Nelson		None	N/A
5	NB Power Corporation	Laura McLeod		Abstain	N/A
5	Nebraska Public Power District	Don Schmit		Abstain	N/A
5	New York Power Authority	Randy Crissman		Affirmative	N/A
5	NextEra Energy	Allen Schriver		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	NiSource - Northern Indiana Public Service Co.	Dmitriy Bazylyuk		Affirmative	N/A
5	Northern California Power Agency	Marty Hostler		None	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	John Rhea		None	N/A
5	Omaha Public Power District	Mahmood Safi		Negative	Comments Submitted
5	Ontario Power Generation Inc.	David Ramkalawan		Affirmative	N/A
5	OTP - Otter Tail Power Company	Cathy Fogale		Negative	Comments Submitted
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	JULIE HOSTRANDER		None	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A
5	Public Utility District No. 1 of Chelan County	Haley Sousa		Negative	Comments Submitted
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Negative	Comments Submitted
5	Puget Sound Energy, Inc.	Eleanor Ewry		Affirmative	N/A
5	Sacramento Municipal Utility District	Susan Oto	Joe Tarantino	Negative	Comments Submitted
5	Salt River Project	Kevin Nielsen		Negative	Comments Submitted
5	Santee Cooper	Tommy Curtis		Abstain	N/A
5	SCANA - South Carolina Electric and Gas Co.	Alyssa Hubbard		None	N/A
5	Seattle City Light	Mike Haynes		Negative	Comments Submitted
5	Seminole Electric Cooperative, Inc.	Brenda Atkins		None	N/A
5	Sempra - San Diego Gas and Electric	Jerome Gobby	Andrey Komissarov	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Silicon Valley Power - City of Santa Clara	Sandra Pacheco		None	N/A
5	Southern Company - Southern Company Generation	William D. Shultz		Affirmative	N/A
5	SunPower	Bradley Collard		None	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin		Negative	Comments Submitted
5	Talen Generation, LLC	Matthew McMillan		None	N/A
5	TECO - Tampa Electric Co.	Frank L Busot		None	N/A
5	Tennessee Valley Authority	M Lee Thomas		Abstain	N/A
5	U.S. Bureau of Reclamation	Wendy Center		Negative	Comments Submitted
5	Westar Energy	Laura Cox		Affirmative	N/A
6	APS - Arizona Public Service Co.	Jonathan Aragon		Affirmative	N/A
6	Arkansas Electric Cooperative Corporation	Bruce Walkup		None	N/A
6	Austin Energy	Andrew Gallo		Affirmative	N/A
6	Basin Electric Power Cooperative	Paul Huettl		Affirmative	N/A
6	Berkshire Hathaway - PacifiCorp	Sandra Shaffer		Negative	Comments Submitted
6	Cleco Corporation	Robert Hirchak	Louis Guidry	Abstain	N/A
6	Con Ed - Consolidated Edison Co. of New York	Robert Winston		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
6	Duke Energy	Greg Cecil		Affirmative	N/A
6	Edison International - Southern California Edison Company	Kenya Streeter		None	N/A
6	Entergy	Julie Hall		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Exelon	Becky Webb		Abstain	N/A
6	FirstEnergy - FirstEnergy Solutions	Ann Ivanc		Affirmative	N/A
6	Florida Municipal Power Pool	Tom Reedy	Brandon McCormick	Affirmative	N/A
6	Great Plains Energy - Kansas City Power and Light Co.	Jim Flucke	Douglas Webb	Affirmative	N/A
6	Lincoln Electric System	Eric Ruskamp		Negative	Comments Submitted
6	Los Angeles Department of Water and Power	Anton Vu		Affirmative	N/A
6	Luminant - Luminant Energy	Brenda Hampton		Affirmative	N/A
6	Manitoba Hydro	Blair Mukanik		Affirmative	N/A
6	Muscatine Power and Water	Ryan Streck		Negative	Comments Submitted
6	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		None	N/A
6	NiSource - Northern Indiana Public Service Co.	Joe O'Brien		Affirmative	N/A
6	Northern California Power Agency	Dennis Sismaet		None	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay		None	N/A
6	Omaha Public Power District	Joel Robles		None	N/A
6	Portland General Electric Co.	Daniel Mason		Abstain	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		None	N/A
6	Public Utility District No. 1 of Chelan County	Janis Weddle		Negative	Comments Submitted
6	Public Utility District No. 2 of Grant County, Washington	LeRoy Patterson		None	N/A
6	Sacramento Municipal Utility District	Jamie Cutlip	Joe Tarantino	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Salt River Project	Bobby Olsen		Negative	Comments Submitted
6	Santee Cooper	Michael Brown		Abstain	N/A
6	Seattle City Light	Charles Freeman		Negative	Comments Submitted
6	Seminole Electric Cooperative, Inc.	Trudy Novak		Negative	Comments Submitted
6	Snohomish County PUD No. 1	Franklin Lu		None	N/A
6	Southern Company - Southern Company Generation and Energy Marketing	Jennifer Sykes		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Rick Applegate		Negative	Comments Submitted
6	Talen Energy Marketing, LLC	Jennifer Hohenshilt		None	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		Affirmative	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Abstain	N/A
6	WEC Energy Group, Inc.	Scott Hoggatt		Affirmative	N/A
6	Westar Energy	Megan Wagner		Affirmative	N/A
7	Exxon Mobil	Jay Barnett		None	N/A
7	Luminant Mining Company LLC	Stewart Rake		Affirmative	N/A
8	David Kiguel	David Kiguel		Affirmative	N/A
8	Massachusetts Attorney General	Frederick Plett		Affirmative	N/A
8	Roger Zaklukiewicz	Roger Zaklukiewicz		Affirmative	N/A
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson		Affirmative	N/A
10	Midwest Reliability Organization	Russel Mountjoy		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	New York State Reliability Council	ALAN ADAMSON		Affirmative	N/A
10	Northeast Power Coordinating Council	Guy V. Zito		Affirmative	N/A
10	ReliabilityFirst	Anthony Jablonski		Affirmative	N/A
10	SERC Reliability Corporation	Drew Slabaugh		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Abstain	N/A

Previous 1 Next

Showing 1 to 290 of 290 entries

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2016-02 Modifications to CIP Standards

Formal Comment Period Open through December 11, 2017

Now Available

A 45-day formal comment period for **CIP-012-1 - Cyber Security – Communications between Control Centers** is open through **8 p.m. Eastern, Monday, December 11, 2017.**

The standard drafting team's considerations of the responses received from the last comment period are reflected in this draft of the standard.

Commenting

Use the Standards Balloting and Commenting System (SBS) to submit comments. If you experience issues navigating the SBS, contact Wendy Muller. An unofficial Word version of the comment form is posted on the project page.

- *If you are having difficulty accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out, contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern).*
- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*
- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Next Steps

An additional ballot for the standard and non-binding poll of the associated Violation Risk Factors and Violation Severity Levels will be conducted **December 1-11, 2017**.

For information on the Standards Development Process, refer to the Standard Processes Manual**.**

For more information or assistance, contact Katherine Street at (404) 446-9702 or Mat Bunch at (404) 446-9785.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Comment Report

Project Name:	2016-02 Modifications to CIP Standards | CIP-012-1
Comment Period Start Date:	10/27/2017
Comment Period End Date:	12/11/2017
Associated Ballots:	2016-02 Modifications to CIP Standards CIP-012-1 AB 2 ST

There were 61 sets of responses, including comments from approximately 168 different people from approximately 117 companies representing 10 of the Industry Segments as shown in the table on the following pages.

Questions

1. Requirement R1: The SDT drafted CIP-012-1 Requirement R1 for the Responsible Entity to develop one or more documented plan(s) to mitigate the risk of the unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring and control data while being transmitted between any Control Centers. Do you agree with this revision? If not, please provide the basis for your disagreement and an alternate proposal.

2. Requirement R1: The SDT seeks comment on scoping sensitive BES data as it applies to Real-time Assessment and Real-time monitoring and control data. Do you agree with scoping CIP-012-1 Requirement R1 in this manner? Please provide comment in support of your response.

3. Requirement R2: The SDT drafted CIP-012-1 Requirement R2 for the Responsible Entity to implement the plan(s) specified in Requirement R1, except under CIP Exceptional Circumstances. Do you agree with this revision? If not, please provide the basis for your disagreement and an alternate proposal.

4. Implementation Plan: The SDT revised the Implementation Plan to make the standard effective the first day of the first calendar quarter that is twenty-four (24) calendar months after the effective date of the applicable governmental authority's order approving the standard, or as otherwise provided for by the applicable governmental authority. Do you agree with this proposal? If you think an alternate implementation time period is needed, please provide a detailed explanation of actions and time needed to meet the implementation deadline.

5. The SDT believes proposed CIP-012-1 provides entities with flexibility to meet the reliability objectives in a cost effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost effective approaches, please provide your recommendation and, if appropriate, technical justification.

6. If you have additional comments on the proposed CIP-012-1 – Cyber Security – Communications between Control Centers drafted in response to the FERC directive that you have not provided in response to the questions above, please provide them here.

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim	3	RF	FirstEnergy Corporation	Aaron Ghdooshim	FirstEnergy - FirstEnergy Corporation	4	RF
					Aubrey Short	FirstEnergy - FirstEnergy Corporation	1	RF
					Theresa Ciancio	FirstEnergy - FirstEnergy Corporation	3	RF
					Robert Loy	FirstEnergy - FirstEnergy Solutions	5	RF
					Ann Ivanc	FirstEnergy - FirstEnergy Solutions	6	RF
Southern Company - Southern Company Services, Inc.	Brandon Cain	1,3,5,6	FRCC,MRO,NPCC,SERC,SPP RE,Texas RE,WECC	Southern Company	Katherine Prewitt	Southern Company - Southern Company Services, Inc.	1	SERC
					R. Scott Moore	Southern Company - Alabama Power Company	3	SERC
					William D. Shultz	Southern Company - Southern Company Generation	5	SERC
					Jennifer Sykes	Southern Company - Southern Company Generation and Energy Marketing	6	SERC
Brandon McCormick	Brandon McCormick		FRCC	FMPA	Tim Beyrle	City of New Smyrna Beach Utilities Commission	4	FRCC
					Jim Howard	Lakeland Electric	5	FRCC

					Lynne Mila	City of Clewiston	4	FRCC
					Javier Cisneros	Fort Pierce Utilities Authority	3	FRCC
					Randy Hahn	Ocala Utility Services	3	FRCC
					Don Cuevas	Beaches Energy Services	1	FRCC
					Jeffrey Partington	Keys Energy Services	4	FRCC
					Tom Reedy	Florida Municipal Power Pool	6	FRCC
					Steven Lancaster	Beaches Energy Services	3	FRCC
					Mike Blough	Kissimmee Utility Authority	5	FRCC
					Chris Adkins	City of Leesburg	3	FRCC
					Ginny Beigel	City of Vero Beach	3	FRCC
Tennessee Valley Authority	Brian Millard	1,3,5,6	SERC	Tennessee Valley Authority	Scott, Howell D.	Tennessee Valley Authority	1	SERC
					Grant, Ian S.	Tennessee Valley Authority	3	SERC
					Thomas, M. Lee	Tennessee Valley Authority	5	SERC
					Parsons, Marjorie S.	Tennessee Valley Authority	6	SERC
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
SRC	David Francis	2	FRCC,MRO,NPCC,RF,SERC,SPP RE,Texas RE,WECC	SRC + SWG	Gregory Campoli	New York Independent System Operator	2	NPCC

					Mark Holman	PJM Interconnection, L.L.C.	2	RF
					Charles Yeung	Southwest Power Pool, Inc. (RTO)	2	SPP RE
					Terry BIlke	Midcontinent ISO, Inc.	2	RF
					Elizabeth Axson	Electric Reliability Council of Texas, Inc.	2,3	Texas RE
					Ben Li	IESO	1	MRO
					Drew Bonser	SWG	NA - Not Applicable	NA - Not Applicable
					Darrem Lamb	CAISO	2	WECC
					Matt Goldberg	ISONE	2	NPCC
Seattle City Light	Ginette Lacasse	1,3,4,5,6	WECC	Seattle City Light Ballot Body	Pawel Krupa	Seattle City Light	1	WECC
					Hao Li	Seattle City Light	4	WECC
					Bud (Charles) Freeman	Seattle City Light	6	WECC
					Mike Haynes	Seattle City Light	5	WECC
					Michael Watkins	Seattle City Light	1,4	WECC
					Faz Kasraie	Seattle City Light	5	WECC
					John Clark	Seattle City Light	6	WECC
					Tuan Tran	Seattle City Light	3	WECC
					Laurrie Hammack	Seattle City Light	3	WECC
Public Utility District No. 1 of Chelan County	Janis Weddle	6		Chelan PUD	Haley Sousa	Public Utility District No. 1 of Chelan County	5	WECC
					Joyce Gundry	Public Utility District No. 1 of Chelan County	3	WECC

					Jeff Kimbell	Public Utility District No. 1 of Chelan County	1	WECC
					Janis Weddle	Public Utility District No. 1 of Chelan County	6	WECC
DTE Energy - Detroit Edison Company	Karie Barczak	3,4,5		DTE Energy - DTE Electric	Jeffrey Depriest	DTE Energy - DTE Electric	5	RF
					Daniel Herring	DTE Energy - DTE Electric	4	RF
					Karie Barczak	DTE Energy - DTE Electric	3	RF
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,8,9,10	NPCC	RSC no Dominion and ISO-NE	Guy V. Zito	Northeast Power Coordinating Council	10	NPCC
					Randy MacDonald	New Brunswick Power	2	NPCC
					Wayne Sipperly	New York Power Authority	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	Orange & Rockland Utilities	3	NPCC
					Michele Tondalo	UI	1	NPCC
					Laura Mcleod	NB Power	1	NPCC
					David Ramkalawan	Ontario Power Generation Inc.	5	NPCC
					Quintin Lee	Eversource Energy	1	NPCC
					Paul Malozewski	Hydro One Networks, Inc.	3	NPCC

					Helen Lainis	IESO	2	NPCC
					Michael Schiavone	National Grid	1	NPCC
					Michael Jones	National Grid	3	NPCC
					Greg Campoli	NYISO	2	NPCC
					Sylvain Clermont	Hydro Quebec	1	NPCC
					Chantal Mazza	Hydro Quebec	2	NPCC
					Silvia Mitchell	NextEra Energy - Florida Power and Light Co.	6	NPCC
					Michael Forte	Con Ed - Consolidated Edison	1	NPCC
					Daniel Grinkevich	Con Ed - Consolidated Edison Co. of New York	1	NPCC
					Peter Yost	Con Ed - Consolidated Edison Co. of New York	3	NPCC
					Brian O'Boyle	Con Ed - Consolidated Edison	5	NPCC
					Sean Cavote	PSEG	4	NPCC
Midwest Reliability Organization	Russel Mountjoy	10		MRO NSRF	Joseph DePoorter	Madison Gas & Electric	3,4,5,6	MRO
					Larry Heckert	Alliant Energy	4	MRO
					Amy Casucelli	Xcel Energy	1,3,5,6	MRO
					Michael Brytowski	Great River Energy	1,3,5,6	MRO
					Jodi Jensen	Western Area Power Administratino	1,6	MRO
					Kayleigh Wilkerson	Lincoln Electric System	1,3,5,6	MRO
					Mahmood Safi	Omaha Public Power District	1,3,5,6	MRO

					Brad Parret	Minnesota Power	1,5	MRO
					Terry Harbour	MidAmerican Energy Company	1,3	MRO
					Tom Breene	Wisconsin Public Service	3,5,6	MRO
					Jeremy Volls	Basin Electric Power Coop	1	MRO
					Kevin Lyons	Central Iowa Power Cooperative	1	MRO
					Mike Morrow	Midcontinent Independent System Operator	2	MRO
Dominion - Dominion Resources, Inc.	Sean Bodkin	6		Dominion	Connie Lowe	Dominion - Dominion Resources, Inc.	3	NA - Not Applicable
					Lou Oberski	Dominion - Dominion Resources, Inc.	5	NA - Not Applicable
					Larry Nash	Dominion - Dominion Virginia Power	1	NA - Not Applicable
PSEG	Sean Cavote	1,3,5,6	NPCC,RF	PSEG REs	Tim Kucey	PSEG - PSEG Fossil LLC	5	NPCC
					Karla Barton	PSEG - PSEG Energy Resources and Trade LLC	6	RF
					Jeffrey Mueller	PSEG - Public Service Electric and Gas Co.	3	RF
					Joseph Smith	PSEG - Public Service Electric and Gas Co.	1	RF
Southwest Power Pool, Inc. (RTO)	Shannon Mickens	2	SPP RE	SPP Standards Review Group	Shannon Mickens	Southwest Power Pool Inc.	2	SPP RE
					Megan Wagner	Westar Energy	6	SPP RE
					Louis Guidry	Cleco Corporation	1,3,5,6	SPP RE
					Robert Gray	Board of Public Utilities (BPU),	NA - Not Applicable	NA - Not Applicable

						Kansas City, KS		
					Ron Spicer	EDF Renewables	5	SPP RE
PPL - Louisville Gas and Electric Co.	Shelby Wade	1,3,5,6	RF,SERC	PPL NERC Registered Affiliates	Charlie Freibert	LG&E and KU Energy, LLC	3	SERC
					Brenda Truhe	PPL Electric Utilities Corporation	1	RF
					Dan Wilson	LG&E and KU Energy, LLC	5	SERC
					Linn Oelker	LG&E and KU Energy, LLC	6	SERC

1. Requirement R1: The SDT drafted CIP-012-1 Requirement R1 for the Responsible Entity to develop one or more documented plan(s) to mitigate the risk of the unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring and control data while being transmitted between any Control Centers. Do you agree with this revision? If not, please provide the basis for your disagreement and an alternate proposal.

Kristine Ward - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC

Answer	No
Document Name	

Comment

Comments: The standard would be more effective if it more specifically identified the security objective described in FERC Order No. 822 paragraph 54, of “maintaining the integrity and availability of sensitive BES data”.

With regard to R1.3, the standard should better reflect FERC Order No. 822 paragraph 55, specifically to address that protections should not adversely affect BES reliability, should account for the risk of *CYBE*R assets, and that the information being protected should be results –based and not zero-defect.

Likes 0	
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion

Answer	No
Document Name	

Comment

Dominion Energy recommends changing Measure M1 to the following:

“Evidence may include, but is not limited to, documented plan(s) that meet the criteria identified in Requirement R1.”

Likes 0	
Dislikes 0	

Response

Janis Weddle - Public Utility District No. 1 of Chelan County - 6, Group Name Chelan PUD

Answer	No
Document Name	

Comment
CHPD is generally in agreement with the Draft 2 revision. However; we request that the newly-introduced terms “monitoring data” and “control data” either be replaced by “BES Data” (a new NERC-defined Glossary term) or themselves be defined in the NERC Glossary. Additionally, the concept of “demarcation point(s)” should be constrained to the entity’s equipment, for example “1.2 Identification of *the Responsible Entity’s* demarcation point(s)…” The current wording implies that each entity should document their local demarcation point and also any demarcation point(s) that exist at each neighboring system. A change to a demarcation point in one system should not create a paperwork or compliance issue for a neighbor or vice versa. Alternatively, consider defining the term “demarcation point” in the NERC glossary and identify the scope within the definition of the term.

Likes 5	Public Utility District No. 1 of Snohomish County, 5, Nietfeld Sam; Snohomish County PUD No. 1, 6, Lu Franklin; Public Utility District No. 1 of Snohomish County, 1, Duong Long; Snohomish County PUD No. 1, 3, Oens Mark; Public Utility District No. 1 of Snohomish County, 4, Martinsen John
Dislikes 0	

Response

Aaron Austin - AEP - 3	
Answer	No
Document Name	

Comment
AEP agrees with the SDT on removal of Operational and Planning data from the scope of the Standard, but feels the data specification remains loose. AEP operates in three markets with three RTOs. Our Balancing Authority has requested market related data as part of the TOP-003-3 implementation data specifications. We feel that this market data is out of scope for CIP-012 and the Standard could be further improved by specifying that market related data does not meet the intent for Real-time Assessment and Real time monitoring and control data. Appropriate exclusion language in the Implementation Guidance and Technical rationale may be satisfactory.

Likes 0	
Dislikes 0	

Response

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	

Comment
BPA appreciates the revisions that the SDT has made based on industry feedback on the initial draft, such as adding demarcation points. BPA reiterates its position as documented in BPA’s SAR and initial draft comments that CIP-012-1 is not necessary. We continue to believe that the objectives can be met by coordinating with existing standards such as CIP-003 and CIP-005. However, if the SDT proceeds with CIP-012-1, BPA remains concerned with the technical feasibility of the standard.

Points of discussion:

- Encryption may not be feasible due to availability concerns. (e.g., failure of encryption keys or latency problems with encryption for availability requirements.)
- Additionally, entities and common carriers use a variety of media to carry traffic, and will undoubtedly use traffic shaping to maintain service levels: routing becomes unpredictable; each packet could take a different route from point A to B.
- Even if a single entity owns the entire communication network, this is still a problem. Modern routing protocols will try to deliver packets over a system with inoperable equipment, severed links, etc. The only remedy is to physically protect the entire communication system in advance of system faults to satisfy CIP-012. If one packet traverses a link due to a system fault that is not protected – it would be a violation.

Likes 0	
Dislikes 0	

Response

Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF

Answer	No
Document Name	

Comment

The NSRF does not agree with two separate requirements, one for a plan and one to implementation. We recommend following precedent in the other CIP standards, for example, CIP-004-6. The obligation can be accomplished with one requirement, as follows.

R1. “The Responsible Entity shall implement one or more documented process(es) to mitigate the risk of the unauthorized disclosure or modification of Real-time Assessments and Real-time monitoring and control data while being transmitted between any Control Centers, except under CIP Exceptional Circumstances. This excludes oral communications. The process(es) shall identify:

R1.1 security protection used to mitigate risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring and control data while being transmitted between Control Centers,

R1.2 demarcation point(s) where security protection is applied for transmitting Real-time Assessment and Real-time monitoring and control data between Control Centers. Demarcation points identified by the Responsible Entity do not add additional Cyber Assets to the scope of the CIP Reliability Standards; and

For R1.3, please see our rational in question 6. R1.3 Identify each Responsible Entity for applying security protection(s) to the transmission of Real-time Assessment and Real-time monitoring and control data between Control Centers, when the Control Centers are owned or operated by different Responsible Entities.”

This also includes important scoping from the implementation guidance that belongs in the requirement, that demarcation points don’t add additional Cyber Assets to the scope of the CIP standards.

Likes 0	
Dislikes 0	

Response

Donald Lock - Talen Generation, LLC - 5	
Answer	No
Document Name	
Comment	
We have no technical concerns with the proposed standard, but it is unclear how 3rd party-owned Control Centers that GO/GOPs use through an agency relationship are to be addressed. CIP-012-1 states in sect. 4.1, “The requirements in this standard apply to the following functional entities, referred to as ‘Responsible Entities,’ that own or operate a Control Center,”… “4.1.2. Generator Operator,”…”4.1.3. Generator Owner.” GO/GOPs do not operate agency-relationship Control Centers any more than they own them, so CIP-012-1 responsibilities apparently rest with the owners of 3rd-party Control Centers and not with the GO/GOPs that hire them. It is unclear how these obligations are communicated and administered, however, since 3rd-party Control Center owners are not (and cannot be) NERC-registered entities.	
Likes 0	
Dislikes 0	
Response	
Paul Huettl - Basin Electric Power Cooperative - 6	
Answer	No
Document Name	
Comment	
Please refer to NRECA comments.	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	No
Document Name	
Comment	
Reclamation disagrees that having a plan adds to the reliability of protecting data used for Operational Planning Analysis, Real-time Assessment, and Real-time monitoring. A plan is an unwarranted layer of compliance that is not needed and the present proposed language is too broad and could be interpreted to apply to data or Control Centers over which an entity has no influence. Reclamation recommends the SDT implement the following:	

- Clearly specify that each Responsible Entity is required to mitigate the risk of unauthorized disclosure or modification of **its own** BES Data between **its own** BES Control Centers.

Replace the term “plan” with “process,” and specify the requirements pertain to BES Data and Control Centers.

- Change Requirement R1:

from: The Responsible Entity shall develop one or more documented plan(s) to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring and control data while being transmitted between any Control Centers. This requirement excludes oral communications.

to: Each Responsible Entity shall have one or more documented processes in place to mitigate the risk of unauthorized disclosure or modification of BES Data being transmitted between its own Control Centers. This requirement excludes oral and non-electronic communications.

- Add the following definitions to the NERC Glossary of Terms:

BES Data: BES reliability operating services information related to the entity’s high and medium impact Control Centers which affects Operational Planning Analysis, Real-time Assessments, and Real-time monitoring and control of the facility, and would affect the operation of the BES if compromised.

Likes 0	
Dislikes 0	

Response

Andrew Gallo - Austin Energy - 6

Answer	No
Document Name	

Comment

Austin Energy (AE) agrees the referenced data deserves protection to ensure it has not been modified and FERC directed NERC to “specify how the confidentiality, integrity, and availability of...data should be protected while...transmitted.” However, AE disagrees with the extent to which the proposed standard requires the data be protected. FERC Order 822 states (on page 36), “…we recognize that not all communication network components and data pose the same risk to bulk electric system reliability and may not require the same level of protection.” The proposed standard applies the same protection criteria across all in-scope data. AE does not agree viewing Real-time Assessment and monitoring/control data without context will adversely affect the reliability of the BES. Confidentiality need not be protected for all in-scope data.

Additionally, AE realizes the SDT does not specifying controls to protect confidentiality and integrity, but the only method available to achieve the proposed requirement is encryption. FERC Order 822 states (on page 39), “it is reasonable to conclude that any lag in communication speed resulting from implementation of protections [encryption technologies] should only be measureable on the order of milliseconds and, therefore, will not adversely impact Control Center communications,” but AE believes that statement refers only to a single data stream. Encryption of multiple data streams at once - from one to many points, - may add latency require more computing resources.

Likes 0	
Dislikes 0	

Response

Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	
Comment	

N&ST is concerned with the fact the draft Implementation Guidance for CIP-012 describes a scenario in which BES Control Centers are exchanging data with a “3rd party” (Figure 4, “Network Diagram depicting communications through a 3rd party”). Although the SDT clearly believes that such communications would be in scope for CIP-012 R1, it is N&ST’s opinion that as presently written, R1 would *not* apply. Figure 4 depicts two Control Centers communicating with a 3rd party, not with each other.

Suggested rewording: REPLACE: “...develop one or more documented plan(s) to mitigate the risk of the unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring and control data while being transmitted between any Control Centers.”

WITH: “...develop one or more documented plan(s) to mitigate the risk of the unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring and control data while being transmitted between (1) any two Control Centers, or (2) between a Control Center and a third-party that provides Real-time Assessment data.”

Likes 0	
Dislikes 0	
Response	

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	No
Document Name	
Comment	

The SPP Standards Review Group appreciates the time and effort expended by the drafting team to further this effort and supports the current standard’s development as an objective based standard, rather than as a prescriptive based standard.

The SPP Standards Review Group appreciates the time and effort expended by the drafting team to further this effort and supports the current standard’s development as an objective based standard, rather than as a prescriptive based standard. The SPP Standards Review Group would recommend a formal definition for “Demarcation Point” be included in the NERC Glossary of Terms and define the protection, if required. Additionally, the SPP Standards Review Group requests clarification whether Demarcation Points need to be classified as CIP Assets or just identified in the documented plan(s)?

Likes 0	
Dislikes 0	
Response	

Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	No
Document Name	
Comment	
NRECA supports the structure of R1 and we appreciate the removal of “data used for Operational Planning Analysis” language. However, new language was also added to R1 and we are unsure of what qualifies as “control data” as used in this requirement. NRECA reviewed the related draft Implementation Guidance and draft Technical Rationale and we did not see any information that explained what “control data” is. Please provide clarity on what “control data” means.	
Likes 0	
Dislikes 0	
Response	

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	
Comment	
We do not agree with two separate requirements, one for a plan and one to implement. We recommend following precedent in the other CIP standards, for example, CIP-004-011. The obligation can be accomplished with one requirement, as follows. “The Responsible Entity shall implement one or more documented process(es) to mitigate the risk of the unauthorized disclosure or modification of Real-time Assessments and Real-time monitoring and control data while being transmitted between any Control Centers, except under CIP Exceptional Circumstances. This excludes oral communications. The process(es) shall identify: 1.1 security protection used to mitigate risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring and control data while being transmitted between Control Centers. 1.2 demarcation point(s) where security protection is applied for transmitting Real-time Assessment and Real-time monitoring and control data between Control Centers. Demarcation points identified by the Responsible Entity do not add additional Cyber Assets to the scope of the CIP Reliability Standards; and 1.3 roles and responsibilities of each Responsible Entity for applying security protection to the transmission of Real-time Assessment and Real-time monitoring and control data between Control Centers, when the Control Centers are owned or operated by different Responsible Entities.” This also includes important scoping from the implementation guidance that belongs in the requirement, that demarcation points don’t add additional Cyber Assets to the scope of the CIP standards.	
Likes 0	
Dislikes 0	
Response	

Lona Calderon - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	

SRP agrees the data should be protected. SRP also agrees the protections for the data in scope must ensure the data has not been modified, and that FERC directed NERC to “specify how the confidentiality, integrity, and availability of each type of bulk electric system data should be protected while it is being transmitted.” However, SRP takes exception to the extent the proposed standard requires the data in scope to be protected. FERC Order 822 states on page 36, “…we recognize that not all communication network components and data pose the same risk to bulk electric system reliability and may not require the same level of protection.” However, the proposed standard applies the same criteria of protection against unauthorized disclosure across all of the data within the defined scope. SRP does not agree viewing of the Real-time Assessment and Real-time monitoring and control data without context will decrease the reliable operation of the BES and asserts confidentiality does not need to be protected for all data under this scope.

Additionally, SRP recognizes the SDT is not specifying the controls used to protect confidentiality and integrity. However, the only method available to achieve the proposed required objective is to implement encryption. FERC Order 822 states on page 39, “it is reasonable to conclude that any lag in communication speed resulting from implementation of protections [encryption technologies] should only be measureable on the order of milliseconds and, therefore, will not adversely impact Control Center communications,” but SRP asserts this statement only refers to a single data stream. It is unknown what encryption will do when dealing with multiple data streams being transmitted at once, from one to many points, not only to the latency added for the reliable operation of the BES, but also to the computing resources.

Likes 0	
Dislikes 0	

Response

Annette Johnston - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3

Answer	No
Document Name	

Comment

Support Terry Harbour comments (Berhshire Hathaway - MidAmerican Energy Company)

Likes 0	
Dislikes 0	

Response

Oshani Pathirane - Oshani Pathirane On Behalf of: Payam Farahbakhsh, Hydro One Networks, Inc., 1, 3; - Oshani Pathirane

Answer	No
Document Name	

Comment

While Hydro One supports the general intent of the Standard, we request that our suggestions below are incorporated. We do not agree with the addition of R1.3. We believe that this wording does not sufficiently address potential disagreements between entities. The Standard should address a situation in which two entities at each end of a communication link cannot reach an agreement on the level of protection that needs to be applied to the communication link between their Control Centres, or, the situation in which one entity’s plan does not align with another entity’s plan.

In addition, it is not clear how the Standard addresses Control Centres that will be built in the future. The term “plan” and verbiage of Requirement 1 suggests that this may be a one-time plan that will address existing Control Centres only.

An alternative approach may be to remove the word “plan” and simply require entities to implement logical/physical controls that both entities agree upon. If the entities cannot reach an agreement, a third party can be selected to provide a resolution.

In addition, the measures (M1) do not sufficiently describe how compliance would be demonstrated.

Likes 0	
Dislikes 0	

Response

Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	No
Document Name	

Comment

No, CenterPoint Energy Houston Electric, LLC (“CenterPoint Energy”) does not agree with this revision. CenterPoint Energy recommends the following revisions to proposed Requirement R1:

The Responsible Entity shall develop one or more documented plan(s) to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers. This requirement excludes oral communications. The plan shall include: [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].

CenterPoint Energy recommends the SDT remove the phrase “and control” from the expanded phrase “Real-time monitoring and control data.” The inclusion of the phrase “and control” may create confusion and does not align with TOP-003 and IRO-010 data specification Requirements. Additionally, the phrase was not mentioned in FERC Order 822. The SDT recognizes in the corresponding Technical Rationale document that “in practice Real-time control data is not transmitted separately from Real-time monitoring data.” Given this practice, the introduction of the concept of separately transmitted “Real-time control data” may create confusion on whether there are additional data specification responsibilities besides those detailed in TOP-003 and IRO-010. Additionally, when control signals that result in the physical operation of BES elements are transmitted between Control Centers, such control signals receive the same protection from unauthorized disclosure or modification as the data and information identified as necessary to perform Real-time Assessments and Real-time monitoring. Thus, there is no need for the additional language to the phrase and no additional benefit to the industry or Reliability.

CenterPoint Energy also recommends removing the word “any” from the phrase “any Control Center” because the word is too broad and does not add value or clarity to the requirement.

CenterPoint Energy also notes that the definition of Control Center is currently being revised. CenterPoint Energy recommends that the definition of Control Center be finalized before the final ballot of CIP-012-1.

Likes 0	

Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	No
Document Name	

Comment

While the SDT believes the “integrity and availability of sensitive bulk electric system data”, as noted in FERC Order No. 822, paragraph 54, is addressed in R1, Texas RE notes the use of the term “or”: Identification of security protection used to mitigate the risk of unauthorized disclosure **or** modification of Real-time Assessment and Real-time monitoring and control data while being transmitted between Control Centers. In its response, the SDT specifically referenced the Consideration of Issue or Directive document. In that document, the SDT makes clear that entities may elect, solely at their discretion, to protect communications links, data, or both.

Texas RE believes this directly conflicts with the plain language in FERC Order No. 822, P. 54. FERC made it clear that protections should apply to both communication links and sensitive data. However, the SDT has specified such protections could be potentially applied solely to communications links or sensitive data. That is, the SDT has endorsed permitting responsible entities to simply elect to plan and implement physical protections for communications links. This would “mitigate” the risk of an unauthorized disclosure or modification of data using one of the delineated methods. As such, the responsible entity would potentially be compliant with the standard without proposing or implementing any logical protections for sensitive data during its transmission. This appears counter to FERC’s intent to protect “**both** the integrity and availability of sensitive bulk electric system data.” FERC Order No. 822, P. 54. Texas RE maintains its recommendation to 1) change “or” to “and”; and 2) change the phrase risk of unauthorized disclosure or modification to integrity and availability of sensitive bulk electric system data.

Additionally, Since GO does not appear in the definition of Control Center, Texas RE suggests removing GO from the applicability section.

Likes 0	
Dislikes 0	

Response

Jennifer Hohenshilt - Talen Energy Marketing, LLC - 6	
Answer	No
Document Name	

Comment

We have no technical concerns with the proposed standard, but it is unclear how 3rd party-owned Control Centers that GO/GOPs use through an agency relationship are to be addressed. CIP-012-1 states in sect. 4.1, “The requirements in this standard apply to the following functional entities, referred to as ‘Responsible Entities,’ that own or operate a Control Center,”… “4.1.2. Generator Operator,”…”4.1.3. Generator Owner.” GO/GOPs do not operate agency-relationship Control Centers any more than they own them, so CIP-012-1 responsibilities apparently rest with the owners of 3rd-

party Control Centers and not with the GO/GOPs that hire them. It is unclear how these obligations are communicated and administered, however, since 3rd-party Control Center owners are not (and cannot be) NERC-registered entities.	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - Consumers Energy Company - 1,3,4,5 - RF	
Answer	No
Document Name	
Comment	
The requirement as written does not provide clear threshold on the type of Control Centers that should be in scope for this standard, i.e. does this requirement apply to high/medium impact BES Cyber Systems, or it also applies to low impact BES Cyber System. Please clarify. Please also consider how to incorporate the scoping criteria into CIP-002 standard.	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	No
Document Name	
Comment	
We support SRP and Chelan PUD comments.	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino	
Answer	No
Document Name	

Comment
It not clear who will maintain responsibility for compliance with the standard and who will be audited.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	No
Document Name	

Comment
We are still unclear on the included data. For R1.2, recommend that the Entities should mutually agree on the demarcation points. For R1.3, we are concerned with resolution of disagreements between different Entities.

Likes 0	
Dislikes 0	

Response

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5

Answer	No
Document Name	

Comment
It is unnecessary to have 2 Requirements for this Standard, especially with each Requirement currently identified to have the same enforceable date. NV Energy recommends following precedence of other Standards and combining the Requirements into a single requirement that states, "An entity shall implement one or more document processes/plans....". .

Likes 0	
Dislikes 0	

Response

sean erickson - Western Area Power Administration - 1

Answer	No
Document Name	

Comment

WAPA does not agree with two separate requirements, one for a plan and one for implementation. We recommend following precedent in the other CIP standards, for example, CIP-004-6. The obligation can be accomplished with one requirement, as follows.

R1. “The Responsible Entity shall implement one or more documented process(es) to mitigate the risk of the unauthorized disclosure or modification of Real-time Assessments and Real-time monitoring and control data while being transmitted between any Control Centers, except under CIP Exceptional Circumstances. This excludes oral communications. The process(es) shall identify:

R1.1 security protection used to mitigate risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring and control data while being transmitted and received between Control Centers,

R1.2 demarcation point(s) where security protection is applied for transmitting Real-time Assessment and Real-time monitoring and control data between Control Centers. Demarcation points identified by the Responsible Entity do not add additional Cyber Assets to the scope of the CIP Reliability Standards; and

R1.3. Identification of roles and responsibilities of each Responsible Entity for applying security protection to the transmission of Real-time Assessment and Real-time monitoring and control data between Control Centers, when the Control Centers are owned or operated by different Responsible Entities.

Other changes in this recommended language:

R1.1 was changed to clarify that data is being protected while being “transmitted and received” between Control Centers.

R1.2 was changed to include important scoping from the implementation guidance that belongs in the requirement, that demarcation points don’t add additional Cyber Assets to the scope of the CIP standards.

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion and ISO-NE

Answer	No
Document Name	

Comment

We are still unclear on the included data. For R1.2, recommend that the Entities should mutually agree on the demarcation points. For R1.3, we are concerned with resolution of disagreements between different Entities.

Likes 0	
Dislikes 0	

Response

Rick Applegate - Tacoma Public Utilities (Tacoma, WA) - 6	
Answer	No
Document Name	
Comment	

Tacoma Power endorses the draft comments shared with it by Salt River Project (SRP), which follow:

SRP agrees the data should be protected. SRP also agrees the protections for the data in scope must ensure the data has not been modified, and that FERC directed NERC to “specify how the confidentiality, integrity, and availability of each type of bulk electric system data should be protected while it is being transmitted.” However, SRP takes exception to the extent the proposed standard requires the data in scope to be protected. FERC Order 822 states on page 36, “…we recognize that not all communication network components and data pose the same risk to bulk electric system reliability and may not require the same level of protection.” However, the proposed standard applies the same criteria of protection against unauthorized disclosure across all of the data within the defined scope. SRP does not agree viewing of the Real-time Assessment and Real-time monitoring and control data without context will decrease the reliable operation of the BES and asserts confidentiality does not need to be protected for all data under this scope.

Additionally, SRP recognizes the SDT is not specifying the controls used to protect confidentiality and integrity. However, the only method available to achieve the proposed required objective is to implement encryption. FERC Order 822 states on page 39, “it is reasonable to conclude that any lag in communication speed resulting from implementation of protections [encryption technologies] should only be measureable on the order of milliseconds and, therefore, will not adversely impact Control Center communications,” but SRP asserts this statement only refers to a single data stream. It is unknown what encryption will do when dealing with multiple data streams being transmitted at once, from one to many points, not only to the latency added for the reliable operation of the BES, but also to the computing resources.

Likes 0	
Dislikes 0	
Response	

Richard Vine - California ISO - 2	
Answer	Yes
Document Name	
Comment	

The California ISO supports the comments of the IRC Security Working Group (SWG)

Likes 0	
Dislikes 0	
Response	

Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	

Comment	
PSEG agrees with the revision; however, the SDT should clarify that it is permissible for the demarcation point to be located outside the ESP/PSP.	
Likes 4	PSEG - Public Service Electric and Gas Co., 1, Smith Joseph; PSEG - Public Service Electric and Gas Co., 3, Mueller Jeffrey; Long Island Power Authority, 1, Ganley Robert; PSEG - PSEG Fossil LLC, 5, Kucey Tim
Dislikes 0	
Response	
Ronald Donahey - TECO - Tampa Electric Co. - 3	
Answer	Yes
Document Name	
Comment	
TEC wishes to endorse the comment of the Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	
Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 3	
Answer	Yes
Document Name	
Comment	
PNMR Agrees with the SDT and AEP's comments to remove Operational and Planning data from the scope of the Standard. However we do not share AEP’s concerns and comments regarding market related data.	
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 agrees with the revision, however, we feel that in order to ensure consistency throughout the industry, the drafting team should consider developing definitions for Real-time Monitoring and Real-time Control Data. Neither of these terms are NERC defined, and could lead to varying interpretations throughout the industry. Does the Real-time Monitoring data only include the data specified in TOP-003 and IRO-010? Does it include SCADA data used specifically to control field assets like generators (AGC) , circuit breakers, relays, etc.? The standard would be improved with additional clarity around these terms.

Likes 0	
Dislikes 0	

Response

Shannon Fair - Colorado Springs Utilities - 1,3,5,6	
Answer	Yes
Document Name	

Comment
CSU agrees the data should be protected. SRP also agrees the protections for the data in scope must ensure the data has not been modified, and that FERC directed NERC to “specify how the confidentiality, integrity, and availability of each type of bulk electric system data should be protected while it is being transmitted.” However, CSU takes exception to the extent the proposed standard requires the data in scope to be protected. FERC Order 822 states on page 36, “…we recognize that not all communication network components and data pose the same risk to bulk electric system reliability and may not require the same level of protection.” However, the proposed standard applies the same criteria of protection against unauthorized disclosure across all of the data within the defined scope. CSU does not agree viewing of the Real-time Assessment and Real-time monitoring and control data without context will decrease the reliable operation of the BES and asserts confidentiality does not need to be protected for all data under this scope.

Likes 0	
Dislikes 0	

Response

Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE	
Answer	Yes
Document Name	

Comment
Xcel Energy agrees with the removal of language related to Planning Analysis, but continues to have concerns with implementation of this Standards as related to the term and definition of Control Center. Specifically, Xcel Energy is concerenced with the definition of "associated data centeres" as part of the Control Center. The Standard does not appear to apply to communication between the control center and a field device (per reference model on page 5 of Technical Rationale). However, if there is a control center communicating with a device that aggregates multiple field devices, such as a dual ported RTU, is that aggregating device location considered an associated data center?

Likes 0	

Dislikes 0	

Response

Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	

Comment
ERCOT signs onto the comments of the SRC/ITC/SWG of the IRC, pasted below. Comments: The SRC & ITC SWG offers the following comment and recommendation. To draw a more clear line to the TOP-003 and IRO-010 standards, the SWG recommends revising Requirement R1 as follows, “For Real-time Assessment and Real-time monitoring and control data, as documented by a Reliability Coordinator, Transmission Operator, or Balancing Authority, the Responsible Entity shall develop one or more documented plan(s) to mitigate the risk of the unauthorized disclosure or modification of the data while it is being transmitted between Control Centers. This excludes oral communications, regardless of transport means.”

Likes 0	
Dislikes 0	

Response

Chantal Mazza - Hydro-Qu?bec TransEnergie - 2 - NPCC	
Answer	Yes
Document Name	

Comment
R1 addresses developing a plan and R2 implementing the plan. In numerous EOP standards involving plans as well as in IRO-014, the terminology used is “develop, maintain and implement”. Maintenance of a plan i.e. keeping it up to date is essential. Thus we recommend modifying R1 so that it reads : R1. The Responsible Entity shall develop and maintain one or more documented plan(s) to mitigate (…) This comment is more of a comprehension question. If we take for example the following : we have two control centers and the distance between the two control centers is approximately 20 miles (32Km) . One control center has two buildings and the distance between the two buildings is approximately 70 miles (112Km). One building is for the Operating personnel hosting facility, which has a defined PSP and an ESP. The other building, is the data Center (hosting RAS servers), which has a defined PSP and an ESP. There is a communication link (70 miles (112Km)) between the Operating personnel hosting building and the data center building. This communication link would not be subject of CIP-012. The communication link (20 miles (32Km)) between the two control centers would be subject to the CIP-012.

Is this comprehension correct?	
Likes 0	
Dislikes 0	
Response	
Andrey Komissarov - Andrey Komissarov On Behalf of: Jerome Gobby, Sempra - San Diego Gas and Electric, 5, 3, 1; - Andrey Komissarov	
Answer	Yes
Document Name	
Comment	
SDG&E is in agreement with Duke Energy's comments	
Likes 0	
Dislikes 0	
Response	
Laurie Williams - PNM Resources - Public Service Company of New Mexico - 1	
Answer	Yes
Document Name	
Comment	
PNMR Agrees with the SDT and AEP's comments to remove Operational and Planning data from the scope of the Standard. However we do not share AEP's concerns and comments regarding market related data.	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	

Scoping to real-time data is appropriate as entities share significant amounts of data between control centers for coordination, safety, and operations that would not have an 15 minute impact on the BES. The requirement should only apply to real-time data that would impact BES operations.

Likes 0	
Dislikes 0	

Response

David Francis - SRC - 2 - MRO,Texas RE,NPCC,SERC,RF, Group Name SRC + SWG

Answer	Yes
Document Name	

Comment

Comments: The SRC & ITC SWG offers the following comment and recommendation. To draw a more clear line to the TOP-003 and IRO-010 standards, the SWG recommends revising Requirement R1 as follows, “For Real-time Assessment and Real-time monitoring and control data, as documented by a Reliability Coordinator, Transmission Operator, or Balancing Authority, the Responsible Entity shall develop one or more documented plan(s) to mitigate the risk of the unauthorized disclosure or modification of the data while it is being transmitted between Control Centers. This excludes oral communications, regardless of transport means.”

Likes 0	
Dislikes 0	

Response

Steven Powell - Trans Bay Cable LLC - NA - Not Applicable - WECC

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 3, Group Name FirstEnergy Corporation	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eleanor Ewry - Puget Sound Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brandon McCormick - Brandon McCormick On Behalf of: Ginny Beigel, City of Vero Beach, 3; Lynne Mila, City of Clewiston, 4; Tom Reedy, Florida Municipal Power Pool, 6; - Brandon McCormick, Group Name FMPA	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Douglas Webb - Douglas Webb On Behalf of: Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; James McBee, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; Jessica Tucker, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; Jim Flucke, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; - Douglas Webb	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
larry brusseau - Corn Belt Power Cooperative - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
W. Dwayne Preston - Austin Energy - 3	
Answer	
Document Name	
Comment	
I support Andrew Gallo's Comments from Austin Energy.	
Likes 0	
Dislikes 0	
Response	

2. Requirement R1: The SDT seeks comment on scoping sensitive BES data as it applies to Real-time Assessment and Real-time monitoring and control data. Do you agree with scoping CIP-012-1 Requirement R1 in this manner? Please provide comment in support of your response.

sean erickson - Western Area Power Administration - 1

Answer	No
Document Name	

Comment

WAPA agrees with the removal of “data related to Operational Planning Analysis” from R1. However, clarification is needed to ensure that the “control data” term is consistently applied and clearly addresses the intent of FERC’s directive. Additionally, important scoping from the implementation guidance belongs in the requirement, that demarcation points don’t add additional Cyber Assets to the scope of the CIP standards.

Likes 0	
Dislikes 0	

Response

Andrey Komissarov - Andrey Komissarov On Behalf of: Jerome Gobby, Sempra - San Diego Gas and Electric, 5, 3, 1; - Andrey Komissarov

Answer	No
Document Name	

Comment

SDG&E is in agreement with Xcel Energy's comments

Likes 0	
Dislikes 0	

Response

Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino

Answer	No
Document Name	

Comment

We have a concern regarding real time assessment, the real time assessment is a study about the system condition and is not going to change the status of the power system. The data does not need to be protected to this level because knowledge of the data would not lead to scenario that would impact the BES within 15 minutes. Additionally, the operators validate the data through reasonable tests before they make operational actions.

Likes 0	
Dislikes 0	

Response

Jeanne Kurzynowski - Consumers Energy Company - 1,3,4,5 - RF

Answer	No
Document Name	

Comment

Please clarify the scope of the standard and requirement.

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	No
Document Name	

Comment

Texas RE notes the SDT modified R1 to apply to Real-time Assessment (RTA) and Real-time monitoring to be consistent with the definition of Control Center, however, Texas RE recommends including Operational Planning Analysis (OPA). The SDT's position is that OPA data for the next day, if rendered unavailable, would not adversely impact the reliable operation of the BES within 15 minutes. However, impact to the reliable operation of the BES within 15 minutes should not be the only consideration for protection of OPA data. Texas RE notes that OPA and RTA data are distinguishable only by the period that data is actually used. Most important, OPA's data risk of unauthorized disclosure should be mitigated consistent with other similar sensitive data. For example, if a registered entity's communications between Control Centers were compromised, OPA data may be useful in the planning of future attacks on the BES. The OPA data includes information such an evaluation of projected system conditions to assess anticipated (pre-Contingency) and potential (post-Contingency) conditions for next-day operations. The evaluation also reflects load forecasts; generation output levels; Interchange; known Protection System and Special Protection System status or degradation. It is not difficult to think of a scenario whereby unauthorized disclosure of OPA data, may adversely impact the reliable operation of the BES within 15 minutes.

Since the SDT is electing not to directly reference other standards, the SDT could change the language of R1 to say: *The Responsible Entity shall develop one or more documented plan(s) to mitigate the risk of unauthorized disclosure or modification of data as defined by the data specification*

required to fulfill operational and planning responsibilities while being transmitted between any Control Centers. This would make CIP-012-1 consistent with the IRO-010 and TOP-003 Standards, as well as include the OPA data.

Since the terms “Real-time monitoring” and “control data”, used in part 1.3, is not defined, Texas RE requests the SDT provide examples of this type of data. This could be done as part of the Implementation Guidance document.

Texas RE requests the SDT describe the types of controls it expects to see that are not covered by IRO-010 and TOP-003.

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 believes that the types of data to be within scope, as identified by data specification lists orginating from Requirements TOP-003 and IRO-010 are not specific enough to determine or limit the types of data or communciation methods that would need to be protected as Real Time Assessment, Real Time Monitoring, or Control Data. These lists contain data and methods of communicating data that Xcel Energy would not clasify as Real Time Assessment, Real Time Monitoring, or Control Data. Xcel Energy's concern is that NERC and/or Regional Entites may. The inclusion of all data types and methods on these lists could bring systems like corporate email into scope, which Xcel Energy would adamantly oppose. We suggest adding further clarification as to what types of data are included as Real Time Assessment, Real Time Monitoring and Control Data.

Likes 0	
Dislikes 0	

Response

Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	No
Document Name	

Comment

As mentioned in the Response to Question No. 1, the phrase “and control” should be removed from the requirement.

Likes 0	
Dislikes 0	

Response	
Annette Johnston - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	No
Document Name	
Comment	
Support Terry Harbour comments (Berhshire Hathaway - MidAmerican Energy Company)	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	
Comment	
Important scoping from the implementation guidance belongs in the requirement, that demarcation points don't add additional Cyber Assets to the scope of the CIP standards.	
Likes 0	
Dislikes 0	
Response	
Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	No
Document Name	
Comment	
Same comments as question 1 above.	
Likes 0	
Dislikes 0	
Response	

Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	No
Document Name	
Comment	

Reclamation does not agree with the scope of CIP-012-1 Requirement R1.

Reclamation recommends the SDT implement the following:

- Clearly specify that each Responsible Entity is required to mitigate the risk of unauthorized disclosure or modification of **its own** BES Data between **its own** Control Centers.

Add the following definition to the NERC Glossary of Terms:

BES Data: BES reliability operating services information related to the entity's high and medium impact Control Centers which affects Operational Planning Analysis, Real-time Assessments, and Real-time monitoring and control of the facility, and would affect the operation of the BES if compromised.

Likes 0	
Dislikes 0	
Response	

Paul Huettl - Basin Electric Power Cooperative - 6	
Answer	No
Document Name	
Comment	

Please refer to NRECA comments.

Likes 0	
Dislikes 0	
Response	

Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF	
Answer	No
Document Name	
Comment	

We agree with the removal of “data related to Operational Planning Analysis” from R1. However, clarification is needed to ensure that the “control data” term is consistently applied and clearly addresses the intent of FERC’s directive. Additionally, important scoping from the implementation guidance belongs in the requirement, that demarcation points don’t add additional Cyber Assets to the scope of the CIP standards.

Likes 0	
Dislikes 0	

Response

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

While BPA agrees with the exclusion of Operational Planning Analysis from the scope of R1, we still do not agree with the need for CIP-012.

Likes 0	
Dislikes 0	

Response

Janis Weddle - Public Utility District No. 1 of Chelan County - 6, Group Name Chelan PUD

Answer	No
Document Name	

Comment

CHPD requests more formal definition of terms that describe the data in question. Consider a NERC Glossary term of “BES data” (used in this question) to address “monitoring” and “control” data types in a single definition. A potential, admittedly simple, initial definition to consider:

BES Data – Electronic data used by BES Cyber Systems to perform Supervisory Control and Data Acquisition (SCADA).

If the STD believes that monitoring and control data should be defined separately, then CHPD instead requests new NERC Glossary terms for “monitoring data” and “control data” in place of a combined definition.

Likes 5	Public Utility District No. 1 of Snohomish County, 5, Nietfeld Sam; Snohomish County PUD No. 1, 6, Lu Franklin; Public Utility District No. 1 of Snohomish County, 1, Duong Long; Snohomish County PUD No. 1, 3, Oens Mark; Public Utility District No. 1 of Snohomish County, 4, Martinsen John
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	
Comment	
The term “control data” is not defined. Dominion Energy recommends either defining the term or providing additional guidance on its meaning in the GTB. In addition, Part 1.3 is strictly administrative in nature and does not enhance the reliability of the BES. We recommend that this part be removed in its entirety. Finally, Dominion Energy is concerned that the demarcation line between Entities is not clearly defined.	
Likes 0	
Dislikes 0	
Response	
Rick Applegate - Tacoma Public Utilities (Tacoma, WA) - 6	
Answer	Yes
Document Name	
Comment	
Tacoma Power endorses the draft comments shared with it by Salt River Project (SRP), which follow: SRP agrees scoping CIP-012-1 Requirement R1 in this manner and thanks the SDT for the opportunity to comment on the scope. However, as stated in SRP’s response to question 1, SRP does not agree viewing of the Real-time Assessment and Real-time monitoring and control data without context will decrease the reliable operation of the BES and asserts confidentiality does not need to be protected for all data under this scope.	
Likes 0	
Dislikes 0	
Response	
David Francis - SRC - 2 - MRO,Texas RE,NPCC,SERC,RF, Group Name SRC + SWG	
Answer	Yes
Document Name	
Comment	
None	

Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion and ISO-NE	
Answer	Yes
Document Name	
Comment	
We conceptually agree with the scoping but need more details on “monitoring and control data.” We agree with the removal of “Operational Planning Analysis.”	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
We conceptually agree with the scoping but need more details on “monitoring and control data.” We agree with the removal of “Operational Planning Analysis.”	
Likes 0	
Dislikes 0	
Response	
Brandon McCormick - Brandon McCormick On Behalf of: Ginny Beigel, City of Vero Beach, 3; Lynne Mila, City of Clewiston, 4; Tom Reedy, Florida Municipal Power Pool, 6; - Brandon McCormick, Group Name FMPA	
Answer	Yes
Document Name	
Comment	
FMPA agrees with the removal of data used for Operational Planning Analysis	

Likes 0	
Dislikes 0	
Response	
Laurie Williams - PNM Resources - Public Service Company of New Mexico - 1	
Answer	Yes
Document Name	
Comment	
PNMR agrees with the scoping of sensitive BES data to Real-time Assessment and Real-time monitoring and control data. While others have commented a concern regarding a lack of formal NERC Glossary of Terms definition, PNMR does not share this concern. If this concept was used beyond this standard then a formal defined term would be appropriate.	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	Yes
Document Name	
Comment	
We support SRP and Chelan PUD comments.	
Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Sensitive BES data required Real-time Assessments, Real-time Monitoring and Control data is the appropriate scope in CIP-012-1 Requirement R1	
Likes 0	

Dislikes 0	

Response

Shannon Fair - Colorado Springs Utilities - 1,3,5,6	
Answer	Yes
Document Name	

Comment
CSU agrees scoping CIP-012-1 Requirement R1 in this manner and thanks the SDT for the opportunity to comment on the scope. However, as stated in SRP's response to question 1, SRP does not agree viewing of the Real-time Assessment and Real-time monitoring and control data without context will decrease the reliable operation of the BES and asserts confidentiality does not need to be protected for all data under this scope.

Likes 0	
Dislikes 0	

Response

Lona Calderon - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	

Comment
SRP agrees scoping CIP-012-1 Requirement R1 in this manner and thanks the SDT for the opportunity to comment on the scope. However, as stated in SRP's response to question 1, SRP does not agree viewing of the Real-time Assessment and Real-time monitoring and control data without context will decrease the reliable operation of the BES and asserts confidentiality does not need to be protected for all data under this scope.

Likes 0	
Dislikes 0	

Response

Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 3	
Answer	Yes
Document Name	

Comment
PNMR agrees with the scoping of sensitive BES data to Real-time Assessment and Real-time monitoring and control data. While others have commented a concern regarding a lack of formal NERC Glossary of Terms definition, PNMR does not share this concern. If this concept was used beyond this standard then a formal defined term would be appropriate.

Likes 0	
Dislikes 0	
Response	
Andrew Gallo - Austin Energy - 6	
Answer	Yes
Document Name	
Comment	
AE does not, however, agree viewing Real-time Assessment and monitoring/control data without context will adversely affect reliable operation of the BES and believes not all in-scope data requires the same level of confidentiality.	
Likes 0	
Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 3	
Answer	Yes
Document Name	
Comment	
The revised scoping appropriately omits operational planning.	
Likes 0	
Dislikes 0	
Response	
Ronald Donahey - TECO - Tampa Electric Co. - 3	
Answer	Yes
Document Name	
Comment	
TEC wishes to endorse the comment of the Edison Electric Institute.	
Likes 0	
Dislikes 0	

Response	
Richard Vine - California ISO - 2	
Answer	Yes
Document Name	
Comment	
The California ISO supports the comments of the IRC Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
TVA agrees that the proposed scoping of sensitive BES data consistent with existing standards is appropriate. This approach helps clarify what data to protect should the entity choose an application layer protection, and may also aid in identifying the links to which the controls are applied.	
Likes 0	
Dislikes 0	
Response	
Aaron Austin - AEP - 3	
Answer	Yes
Document Name	
Comment	
AEP believes this aligns with CIP-002 identification processes and narrows the scope appropriately.	
Likes 0	
Dislikes 0	
Response	

Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
larry brusseau - Corn Belt Power Cooperative - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb On Behalf of: Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; James McBee, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; Jessica Tucker, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; Jim Flucke, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; - Douglas Webb	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Hohenshilt - Talen Energy Marketing, LLC - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Oshani Pathirane - Oshani Pathirane On Behalf of: Payam Farahbakhsh, Hydro One Networks, Inc., 1, 3; - Oshani Pathirane	
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	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eleanor Ewry - Puget Sound Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	

Likes 2	PSEG - Public Service Electric and Gas Co., 1, Smith Joseph; PSEG - Public Service Electric and Gas Co., 3, Mueller Jeffrey
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 3, Group Name FirstEnergy Corporation	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donald Lock - Talen Generation, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Steven Powell - Trans Bay Cable LLC - NA - Not Applicable - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
W. Dwayne Preston - Austin Energy - 3	
Answer	
Document Name	
Comment	
I support Andrew Gallo's Comments from Austin Energy.	
Likes 0	
Dislikes 0	
Response	

3. Requirement R2: The SDT drafted CIP-012-1 Requirement R2 for the Responsible Entity to implement the plan(s) specified in Requirement R1, except under CIP Exceptional Circumstances. Do you agree with this revision? If not, please provide the basis for your disagreement and an alternate proposal.

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

While BPA agrees with the language of R2, we still do not agree with the need for CIP-012, or with the standard as currently drafted.

Likes 0	
Dislikes 0	

Response

Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF

Answer	No
Document Name	

Comment

The NSRF does not agree with two separate requirements, one for a plan and one to implementation. We recommend following precedent in the other CIP standards, for example, CIP-004-6. The obligation can be accomplished with one requirement, as follows.

R1. “The Responsible Entity shall implement one or more documented process(es) to mitigate the risk of the unauthorized disclosure or modification of Real-time Assessments and Real-time monitoring and control data while being transmitted between any Control Centers, except under CIP Exceptional Circumstances. This excludes oral communications. The process(es) shall identify:

R1.1 security protection used to mitigate risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring and control data while being transmitted between Control Centers,

R1.2 demarcation point(s) where security protection is applied for transmitting Real-time Assessment and Real-time monitoring and control data between Control Centers. Demarcation points identified by the Responsible Entity do not add additional Cyber Assets to the scope of the CIP Reliability Standards; and

For R1.3, please see our rational in question 6. R1.3 Identify each Responsible Entity for applying security protection(s) to the transmission of Real-time Assessment and Real-time monitoring and control data between Control Centers, when the Control Centers are owned or operated by different Responsible Entities.”

This also includes important scoping from the implementation guidance that belongs in the requirement, that demarcation points don’t add additional Cyber Assets to the scope of the CIP standards.

Likes 0	
Dislikes 0	

Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	No
Document Name	
Comment	

Reclamation recommends the SDT implement the following:

- Replace the term “plan” with “process” for consistency with other CIP standards.
- Change Requirement R2:

from: The Responsible Entity shall implement the plan(s) specified in Requirement R1, except under CIP Exceptional Circumstances

to: The Responsible Entity shall implement the process(s) specified in Requirement R1, except under CIP Exceptional Circumstances

Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	
Comment	

We do not agree with two separate requirements, one for a plan and one to implement. We recommend following precedent in the other CIP standards, for example, CIP-004-011. The obligation can be accomplished with one requirement, as follows. “The Responsible Entity shall implement one or more documented process(es) to mitigate the risk of the unauthorized disclosure or modification of Real-time Assessments and Real-time monitoring and control data while being transmitted between any Control Centers, except under CIP Exceptional Circumstances. This excludes oral communications. The process(es) shall identify: 1.1 security protection used to mitigate risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring and control data while being transmitted between Control Centers. 1.2 demarcation point(s) where security protection is applied for transmitting Real-time Assessment and Real-time monitoring and control data between Control Centers. Demarcation points identified by the Responsible Entity do not add additional Cyber Assets to the scope of the CIP Reliability Standards; and 1.3 roles and responsibilities of each Responsible Entity for applying security protection to the transmission of Real-time Assessment and Real-time monitoring and control data between Control Centers, when the Control Centers are owned or operated by different Responsible Entities.” This also includes important scoping from the implementation guidance that belongs in the requirement, that demarcation points don’t add additional Cyber Assets to the scope of the CIP standards.

Likes 0	
Dislikes 0	
Response	

Annette Johnston - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	No
Document Name	
Comment	
Support Terry Harbour comments (Berhshire Hathaway - MidAmerican Energy Company)	
Likes 0	
Dislikes 0	
Response	
Oshani Pathirane - Oshani Pathirane On Behalf of: Payam Farahbakhsh, Hydro One Networks, Inc., 1, 3; - Oshani Pathirane	
Answer	No
Document Name	
Comment	
We require clarity on how the implementation plan will address Control Centres that will be built in the future.	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	No
Document Name	
Comment	
Texas RE appreciates the SDT's response. As Texas RE previously noted, it does not necessarily oppose a CIP Exceptional Circumstances exception from the implementation requirements set forth in CIP-012-1 R2. However, despite the SDT's response, it remains unclear why certain CIP exception conditions, such as an imminent hardware failure, should necessarily trigger a relaxation of physical security protections for communications links transmitted sensitive data in all circumstances.	
Likes 0	
Dislikes 0	
Response	

Jeanne Kurzynowski - Consumers Energy Company - 1,3,4,5 - RF	
Answer	No
Document Name	
Comment	
Requirement R2 can be combined with Requirement R1 so that it is written in a consistent approach with other FERC approved CIP requirements.	
Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	
Comment	
It is unnecessary to have 2 Requirements for this Standard, especially with each Requirement currently identified to have the same enforceable date. NV Energy recommends following precedence of other Standards and combining the Requirements into a single requirement that states, "An entity shall implement one or more document processes/plans....". .	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1	
Answer	No
Document Name	
Comment	
WAPA does not agree with two separate requirements, one for a plan and one for implementation. We recommend following precedent in the other CIP standards, for example, CIP-004-6. The obligation can be accomplished with one requirement. See response to question 1.	
Likes 0	
Dislikes 0	
Response	

Paul Huettl - Basin Electric Power Cooperative - 6	
Answer	Yes
Document Name	
Comment	
Please refer to NRECA comments.	
Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	Yes
Document Name	
Comment	
The California ISO supports the comments of the IRC Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
A plan would be created to outline protections and classify BES data moving between control centers.	
Likes 0	
Dislikes 0	
Response	
Lona Calderon - Salt River Project - 1,3,5,6 - WECC	

Answer	Yes
Document Name	
Comment	
SRP agrees on implementing a plan and agrees a CIP Exceptional Circumstance is in order.	
Likes 0	
Dislikes 0	
Response	
Shannon Fair - Colorado Springs Utilities - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
CSU agrees on implementing a plan and agrees a CIP Exceptional Circumstance is in order.	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	Yes
Document Name	
Comment	
We support SRP and Chelan PUD comments.	
Likes 0	
Dislikes 0	
Response	
David Francis - SRC - 2 - MRO,Texas RE,NPCC,SERC,RF, Group Name SRC + SWG	
Answer	Yes
Document Name	

Comment	
None	
Likes 0	
Dislikes 0	
Response	
Steven Powell - Trans Bay Cable LLC - NA - Not Applicable - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Janis Weddle - Public Utility District No. 1 of Chelan County - 6, Group Name Chelan PUD	
Answer	Yes
Document Name	
Comment	
Likes 5	Public Utility District No. 1 of Snohomish County, 5, Nietfeld Sam; Snohomish County PUD No. 1, 6, Lu Franklin; Public Utility District No. 1 of Snohomish County, 1, Duong Long; Snohomish County PUD No. 1, 3, Oens Mark; Public Utility District No. 1 of Snohomish County, 4, Martinsen John
Dislikes 0	
Response	
Aaron Austin - AEP - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donald Lock - Talen Generation, LLC - 5	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 3, Group Name FirstEnergy Corporation	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	
Likes 2	PSEG - Public Service Electric and Gas Co., 1, Smith Joseph; PSEG - Public Service Electric and Gas Co., 3, Mueller Jeffrey
Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Andrew Gallo - Austin Energy - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eleanor Ewry - Puget Sound Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
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	
Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Hohenshilt - Talen Energy Marketing, LLC - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chantal Mazza - Hydro-Qu?bec TransEnergie - 2 - NPCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrey Komissarov - Andrey Komissarov On Behalf of: Jerome Gobby, Sempra - San Diego Gas and Electric, 5, 3, 1; - Andrey Komissarov	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laurie Williams - PNM Resources - Public Service Company of New Mexico - 1	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brandon McCormick - Brandon McCormick On Behalf of: Ginny Beigel, City of Vero Beach, 3; Lynne Mila, City of Clewiston, 4; Tom Reedy, Florida Municipal Power Pool, 6; - Brandon McCormick, Group Name FMPA	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb On Behalf of: Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; James McBee, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; Jessica Tucker, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; Jim Flucke, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; - Douglas Webb	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
larry brusseau - Corn Belt Power Cooperative - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rick Applegate - Tacoma Public Utilities (Tacoma, WA) - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ronald Donahey - TECO - Tampa Electric Co. - 3	
Answer	
Document Name	
Comment	
TEC wishes to endorse the comment of the Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	
W. Dwayne Preston - Austin Energy - 3	
Answer	
Document Name	
Comment	

I support Andrew Gallo's Comments from Austin Energy.

Likes 0	
Dislikes 0	

Response

4. Implementation Plan: The SDT revised the Implementation Plan to make the standard effective the first day of the first calendar quarter that is twenty-four (24) calendar months after the effective date of the applicable governmental authority's order approving the standard, or as otherwise provided for by the applicable governmental authority. Do you agree with this proposal? If you think an alternate implementation time period is needed, please provide a detailed explanation of actions and time needed to meet the implementation deadline.

Rick Applegate - Tacoma Public Utilities (Tacoma, WA) - 6

Answer	No
Document Name	

Comment

Tacoma Power endorses the draft comments shared with it by Salt River Project (SRP), which follow:

Overall, SRP does not agree with twenty-four (24) calendar months for the implementation of Requirements R1 and R2. Although SRP recognizes the SDT is not specifying the controls to be used to protect confidentiality and integrity, the only examples provided in the implementation guidance includes encryption. If there are other methods available to achieve the security objective, SRP asks the SDT to provide them. However, the only method available to achieve the proposed required objective, on the ICCP network, is to implement encryption. As FERC order 822 states on page 37, "if several registered entities have joint responsibility for a cryptographic key management system used between their respective Control Centers, they should have the prerogative to come to a consensus on which organization administers that particular key management system." Furthermore, the FERC order states on page 38, "While responsible entities are required to exchange real-time and operational planning data necessary to operate the bulk electric system using mutually agreeable security protocols, there is no technical specification for how this transfer of information should incorporate mandatory security controls." These are activities and specifications that must be created and agreed upon by all registered entities involved in the data transfer. As such the timeline is reliant on registered entities working together on a common solution and would not be achievable within 24 calendar months.

Additionally, if encryption fails, SRP would lose Real-time Assessment and Real-time monitoring and control data. There are many opportunities for encryption to fail that must be addressed. The implementation of encryption requires a pilot to truly understand and address the mechanisms of failure, the impacts encryption would cause on the exchange of the data, and the computing resources required. A pilot also requires a great amount of coordination to execute, not only within the industry, but may also include carriers, vendors, and possibly third-party encryption key program managers.

Because of the aforementioned reasons and concerns, SRP is recommending a phased implementation for CIP-012-1. A 24 month implementation is appropriate, but only for Requirement R1. The 24 months for R1 would provide time to coordinate and create an industry-wide solution. SRP is proposing the SDT include an additional 12 months for Requirement R2. The additional 12 months would be used for a pilot and course correction if needed, in addition to understanding, formulating, and executing maintenance strategies.

Likes 0	
Dislikes 0	

Response

Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric

Answer	No
Document Name	

Comment

This seems to be an excessively long period of time to implement this proposed standard. The security of real-time data is important and should be prioritized. Yes, entities must communicate and develop joint plans to implement, but allowing a long horizon for implementation will not enable this communication to occur faster.

Likes 0	
Dislikes 0	

Response

sean erickson - Western Area Power Administration - 1

Answer	No
Document Name	

Comment

WAPA recommends an increase to at least three years in order to coordinate with other entities, including specification, design, budgeting, implementation and testing.

Likes 0	
Dislikes 0	

Response

Andrey Komissarov - Andrey Komissarov On Behalf of: Jerome Gobby, Sempra - San Diego Gas and Electric, 5, 3, 1; - Andrey Komissarov

Answer	No
Document Name	

Comment

SDG&E is in agreement with BPA's comments

Likes 0	
Dislikes 0	

Response

Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino

Answer	No
Document Name	

Comment
:Agreements between entities takes time and is it is dependent on items an entity cannot control. We recommend at least 36 months.

Likes 0	
Dislikes 0	

Response

Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body

Answer	No
Document Name	

Comment
We support SRP and Chelan PUD comments.

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 does not agree with the proposed Implementation timeline. We share real time data with Registed Entities (REs) such as the Reliability Coordinators (RCs) including MISO, SPP and PEAK. Additionally, we share data with many utilties with Control Centers across our service territory. Finding a common technological solution to implement the proposed mitigating activities in the Requirements will take a substantial effort of the part of all REs. Once a common technology and all legal agreements between REs are in place, Xcel Energy may still have to purchanse and implement those technology solutions. We suggest that NERC should advise and collaborate with all RCs to agree upon a common technology first and then drive those solutions from the RC down to each utility in scope.

Likes 0	
Dislikes 0	

Response

Annette Johnston - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	No
Document Name	
Comment	
Support Terry Harbour comments (Berhshire Hathaway - MidAmerican Energy Company)	
Likes 0	
Dislikes 0	
Response	
Shannon Fair - Colorado Springs Utilities - 1,3,5,6	
Answer	No
Document Name	
Comment	
Overall, CSU does not agree with twenty-four (24) calendar months for the implementation of Requirements R1 and R2. Although CSU recognizes the SDT is not specifying the controls to be used to protect confidentiality and integrity, the only examples provided in the implementation guidance includes encryption. If there are other methods available to achieve the security objective, we ask the SDT to provide them. However, the only method available to achieve the proposed required objective, on the ICCP network, is to implement encryption. As FERC order 822 states on page 37, “if several registered entities have joint responsibility for a cryptographic key management system used between their respective Control Centers, they should have the prerogative to come to a consensus on which organization administers that particular key management system.” Furthermore, the FERC order states on page 38, “While responsible entities are required to exchange real-time and operational planning data necessary to operate the bulk electric system using mutually agreeable security protocols, there is no technical specification for how this transfer of information should incorporate mandatory security controls.” These are activities and specifications that must be created and agreed upon by all registered entities involved in the data transfer. As such the timeline is reliant on registered entities working together on a common solution and would not be achievable within 24 calendar months. Because of the aforementioned reasons and concerns, CSU is recommending a phased implementation for CIP-012-1. A 24 month implementation is appropriate, but only for Requirement R1. The 24 months for R1 would provide time to coordinate and create an industry-wide solution. SRP is proposing the SDT include an additional 12 months for Requirement R2. The additional 12 months would be used for a pilot and course correction if needed, in addition to understanding, formulating, and executing maintenance strategies.	
Likes 0	
Dislikes 0	
Response	
Lona Calderon - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	

Comment
Overall, SRP does not agree with twenty-four (24) calendar months for the implementation of Requirements R1 and R2. Although SRP recognizes the SDT is not specifying the controls to be used to protect confidentiality and integrity, the only examples provided in the implementation guidance includes encryption. If there are other methods available to achieve the security objective, SRP asks the SDT to provide them. However, the only method available to achieve the proposed required objective, on the ICCP network, is to implement encryption. As FERC order 822 states on page 37, “if several registered entities have joint responsibility for a cryptographic key management system used between their respective Control Centers, they should have the prerogative to come to a consensus on which organization administers that particular key management system.” Furthermore, the FERC order states on page 38, “While responsible entities are required to exchange real-time and operational planning data necessary to operate the bulk electric system using mutually agreeable security protocols, there is no technical specification for how this transfer of information should incorporate mandatory security controls.” These are activities and specifications that must be created and agreed upon by all registered entities involved in the data transfer. As such the timeline is reliant on registered entities working together on a common solution and would not be achievable within 24 calendar months. Additionally, if encryption fails, SRP would lose Real-time Assessment and Real-time monitoring and control data. There are many opportunities for encryption to fail that must be addressed. The implementation of encryption requires a pilot to truly understand and address the mechanisms of failure, the impacts encryption would cause on the exchange of the data, and the computing resources required. A pilot also requires a great amount of coordination to execute, not only within the industry, but may also include carriers, vendors, and possibly third-party encryption key program managers. Because of the aforementioned reasons and concerns, SRP is recommending a phased implementation for CIP-012-1. A 24 month implementation is appropriate, but only for Requirement R1. The 24 months for R1 would provide time to coordinate and create an industry-wide solution. SRP is proposing the SDT include an additional 12 months for Requirement R2. The additional 12 months would be used for a pilot and course correction if needed, in addition to understanding, formulating, and executing maintenance strategies.

Likes 0	
Dislikes 0	

Response

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	

Comment
At least three years are needed to coordinate with other entities, including specification, design, budgeting, implementation and testing.

Likes 0	
Dislikes 0	

Response

Andrew Gallo - Austin Energy - 6	
Answer	No
Document Name	

Comment
Overall, AE does not agree with twenty-four (24) calendar months for R1 and R2. Although AE recognizes the SDT does not specify the controls to protect confidentiality and integrity, the only examples provided in the implementation guidance include encryption. If other methods exist, AE believes the SDT should provide them. The only way to achieve the proposed requirement on the ICCP network is encryption. As FERC Order 822 states (on page 37), “if several registered entities have joint responsibility for a cryptographic key management system used between their respective Control Centers, they should have the prerogative to come to a consensus on which organization administers that particular key management system.” The FERC order also states (on page 38), “While responsible entities are required to exchange real-time and operational planning data necessary to operate the bulk electric system using mutually agreeable security protocols, there is no technical specification for how this transfer of information should incorporate mandatory security controls.” These specifications must be created and agreed upon by all registered entities involved in the data transfer. Consequently, the time to comply depends on registered entities working together on a common solution and will likely take more than 24 months. Additionally, if encryption fails, AE would lose Real-time monitoring and control data. Encryption may fail for many reasons. Implementing encryption should involve a pilot period to assess and address the mechanisms of failure, impacts on data exchange and the requisite computing resources. A pilot also requires coordination, not only for the industry, but also carriers, vendors, and, possibly, third-party encryption key program managers. Consequently, AE recommends a phased implementation for CIP-012-1. A 24 month implementation is appropriate for R1 because it would provide time to coordinate and create an industry-wide solution. AE proposes the SDT grant an extra 12 months for R2 to allow for a pilot and adjustments, if needed.

Likes 0	
Dislikes 0	

Response

Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF	
Answer	No
Document Name	

Comment
The NRSF recommends an increase to at least three years in order to coordinate with other entities, including specification, design, budgeting, implementation and testing.

Likes 0	
Dislikes 0	

Response

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	

Comment

BPA appreciates the increase to 24 months but recommends 36 months due to BPA's large amount of applicable data, access to funds and resources to perform work required.	
Likes 0	
Dislikes 0	
Response	
David Francis - SRC - 2 - MRO,Texas RE,NPCC,SERC,RF, Group Name SRC + SWG	
Answer	Yes
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	
Brandon McCormick - Brandon McCormick On Behalf of: Ginny Beigel, City of Vero Beach, 3; Lynne Mila, City of Clewiston, 4; Tom Reedy, Florida Municipal Power Pool, 6; - Brandon McCormick, Group Name FMPA	
Answer	Yes
Document Name	
Comment	
FMPA supports the additional time this implementation plan provides.	
Likes 0	
Dislikes 0	
Response	
Laurie Williams - PNM Resources - Public Service Company of New Mexico - 1	
Answer	Yes
Document Name	
Comment	

A quick internal review by PNMR SMEs indicates that this implementation plan is reasonable for the proposed standard.

Likes 0	
Dislikes 0	

Response

Barry Lawson - National Rural Electric Cooperative Association - 4

Answer	Yes
Document Name	

Comment

NRECA appreciates the change from 12 months to 24 months in the Implementation Plan.

Likes 0	
Dislikes 0	

Response

Vivian Vo - APS - Arizona Public Service Co. - 3

Answer	Yes
Document Name	

Comment

The period of 24 months will likely be reasonable; however, agreement with neighboring entities poses an unpredictable step in terms of time for completion.

Likes 0	
Dislikes 0	

Response

Richard Vine - California ISO - 2

Answer	Yes
Document Name	

Comment

The California ISO supports the comments of the IRC Security Working Group (SWG)

Likes 0	
Dislikes 0	
Response	
Paul Huettl - Basin Electric Power Cooperative - 6	
Answer	Yes
Document Name	
Comment	
Please refer to NRECA comments.	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
The proposed time period allows entities sufficient time to develop internal plans to implement the enhanced security requirements, negotiate the necessary security changes between entities, and to make appropriate contract adjustments with service providers.	
Likes 0	
Dislikes 0	
Response	
Aaron Austin - AEP - 3	
Answer	Yes
Document Name	
Comment	
AEP believes a 24 month Implementation Plan is adequate provided the TOP-003 and IRO-010 Real-time data and the mutually agreeable security protocols are defined prior to the beginning of the CIP-012 implementation period.	
Likes 0	

Dislikes 0	
Response	
Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
larry brusseau - Corn Belt Power Cooperative - 1	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb On Behalf of: Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; James McBee, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; Jessica Tucker, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; Jim Flucke, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; - Douglas Webb	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chantal Mazza - Hydro-Qu?bec TransEnergie - 2 - NPCC	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Jeanne Kurzynowski - Consumers Energy Company - 1,3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Hohenshilt - Talen Energy Marketing, LLC - 6	
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	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Oshani Pathirane - Oshani Pathirane On Behalf of: Payam Farahbakhsh, Hydro One Networks, Inc., 1, 3; - Oshani Pathirane	
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	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eleanor Ewry - Puget Sound Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	
Likes 2	PSEG - Public Service Electric and Gas Co., 1, Smith Joseph; PSEG - Public Service Electric and Gas Co., 3, Mueller Jeffrey
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 3, Group Name FirstEnergy Corporation	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Donald Lock - Talen Generation, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Janis Weddle - Public Utility District No. 1 of Chelan County - 6, Group Name Chelan PUD	
Answer	Yes
Document Name	
Comment	
Likes 5	Public Utility District No. 1 of Snohomish County, 5, Nietfeld Sam; Snohomish County PUD No. 1, 6, Lu Franklin; Public Utility District No. 1 of Snohomish County, 1, Duong Long; Snohomish County PUD No. 1, 3, Oens Mark; Public Utility District No. 1 of Snohomish County, 4, Martinsen John
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Powell - Trans Bay Cable LLC - NA - Not Applicable - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion and ISO-NE	
Answer	
Document Name	
Comment	
We are concerned about equipment under existing contracts. We suggest a solution similar to CIP-013.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	

Document Name	
Comment	
We are concerned about equipment under existing contracts. We suggest a solution similar to CIP-013.	
Likes 0	
Dislikes 0	
Response	
W. Dwayne Preston - Austin Energy - 3	
Answer	
Document Name	
Comment	
I support Andrew Gallo's Comments from Austin Energy.	
Likes 0	
Dislikes 0	
Response	
Ronald Donahey - TECO - Tampa Electric Co. - 3	
Answer	
Document Name	
Comment	
TEC wishes to endorse the comment of the Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	

5. The SDT believes proposed CIP-012-1 provides entities with flexibility to meet the reliability objectives in a cost effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost effective approaches, please provide your recommendation and, if appropriate, technical justification.

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion

Answer	No
Document Name	

Comment

At this time Dominion Energy has no information to assess the cost of a plan that has yet to be developed.

Likes 0	
Dislikes 0	

Response

Janis Weddle - Public Utility District No. 1 of Chelan County - 6, Group Name Chelan PUD

Answer	No
Document Name	

Comment

CHPD cannot determine if the objectives may be accomplished in a cost-effective manner until further clarification is provided for the terms “monitoring data” and “control data” (separate definitions) or “BES data” (combined definition). CHPD also has concerns with vendor availability, with respect to the system software implementation that will be required for all entities industry-wide. The comments provided by other entities to develop an industry-wide encryption specification is appealing and CHPD believes that would provide a better method for achieving the desired intra-entity security.

Likes 5	Public Utility District No. 1 of Snohomish County, 5, Nietfeld Sam; Snohomish County PUD No. 1, 6, Lu Franklin; Public Utility District No. 1 of Snohomish County, 1, Duong Long; Snohomish County PUD No. 1, 3, Oens Mark; Public Utility District No. 1 of Snohomish County, 4, Martinsen John
Dislikes 0	

Response

Aaron Austin - AEP - 3

Answer	No
Document Name	

Comment

AEP believes communication network security requires “mutually agreed upon: formats, processes for resolving conflicts and security protocols” between entities. However in practice, there is little that is mutually agreed upon in the data specification documents as they

relate to IRO-010 and TOP-003. The Balancing Authority, Transmission Operator and Reliability Coordinator specify the data they want to receive in the manner they want to receive it. Others receiving the requests are obligated to comply. Without additional specificity, most entities will be at the mercy of what their BAs, TOPs and RCs require. AEP believes this dependency creates only the presumption that solutions will be cost effective.

Likes 0	
Dislikes 0	

Response

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

BPA's believes that if the data must be protected throughout the transmission, it would seem that could only be accomplished with encryption. For cases where the existing equipment is not capable of encryption, replacement will be costly and implementation lengthy.

Due to BPA's large amount of applicable data, access to funds and resources to perform work required, the solution will be costly.

Likes 0	
Dislikes 0	

Response

Donald Lock - Talen Generation, LLC - 5

Answer	No
Document Name	

Comment

See our response to question #1

Likes 0	
Dislikes 0	

Response

Andrew Gallo - Austin Energy - 6

Answer	No
Document Name	

Comment
AE does not agree the proposal can be implemented in a cost-effective manner. Encryption is the only available solution to protect in-scope data confidentiality and integrity. If the implementation period remains 24 months, entities will expend more resources and capital than using a phased implementation. A phased implementation provides the ability to ensure the most effective plan and plan more accurately within budget cycles. Also, if encryption fails, AE would lose Real-time monitoring and control data. AE believes a 24 month implementation timeline will impact reliability because many opportunities exist for encryption to fail and those challenges must be addressed, which has a direct affect on cost.

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
We are unable to answer this question in full at this time. The cost of implementation cannot be adequately assessed until discussion and coordination with our neighboring entities (control centers) has taken place. We do not know what additional protections or updates may need to be put in place until said discussions occur.

Likes 0	
Dislikes 0	

Response

Lona Calderon - Salt River Project - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment
SRP does not agree the current standard and implementation plan can be executed in a cost effective manner. Encryption is the only solution available to protect both confidentiality and integrity for the data within this scope. If the implementation timeframe remains at 24 months, more resources and capital will be required versus a phased implementation. A phased implementation provides the ability to not only ensure the most effective plan, but also provides the ability to plan more accurately within budget cycles. More importantly, if encryption fails, SRP would lose Real-time Assessment and Real-time monitoring and control data. SRP is concerned a 24 month implementation timeline would impact reliability as there are many opportunities for encryption to fail that must be addressed. This has a direct correlation on cost when addressing those opportunities during this timeframe.

Likes 0	
Dislikes 0	

Response	
Shannon Fair - Colorado Springs Utilities - 1,3,5,6	
Answer	No
Document Name	
Comment	
CSU does not agree the current standard and implementation plan can be executed in a cost effective manner. Encryption is the only solution available to protect both confidentiality and integrity for the data within this scope. If the implementation timeframe remains at 24 months, more resources and capital will be required versus a phased implementation. A phased implementation provides the ability to not only ensure the most effective plan, but also provides the ability to plan more accurately within budget cycles. More importantly, if encryption fails, CSU would lose Real-time Assessment and Real-time monitoring and control data. CSU is concerned a 24 month implementation timeline would impact reliability as there are many opportunities for encryption to fail that must be addressed. This has a direct correlation on cost when addressing those opportunities during this timeframe.	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE	
Answer	No
Document Name	
Comment	
We believe that the cost effectiveness of implementation would depend on the technology that would need to be deployed. Similar to response to question 4, NERC should advise and work with all RCs to agree upon a common technology and drive those solutions from the RC down to each utility in order to ensure cost effectiveness. The implementation of several different technologies to communicate with several different RCs and utilities would be overly burdensome and at a cost that would not be effective.	
Likes 0	
Dislikes 0	
Response	
Jennifer Hohenshilt - Talen Energy Marketing, LLC - 6	
Answer	No
Document Name	
Comment	

See response to Q1	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - Consumers Energy Company - 1,3,4,5 - RF	
Answer	No
Document Name	
Comment	
More flexibility and less guidance could lead to inconsistency on requirement implementation among different entities.	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	No
Document Name	
Comment	
We support SRP and Chelan PUD comments.	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino	
Answer	No
Document Name	
Comment	

We recommend that an encryption standard is published to guide entities. Developing protocols between entities is time consuming and costly. An exception process can be defined if needed to offer flexibility.

Likes 0	
Dislikes 0	

Response

Andrey Komissarov - Andrey Komissarov On Behalf of: Jerome Gobby, Sempra - San Diego Gas and Electric, 5, 3, 1; - Andrey Komissarov

Answer	No
Document Name	

Comment

SDG&E is in agreement with BPA's comments

Likes 0	
Dislikes 0	

Response

RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC

Answer	No
Document Name	

Comment

SCE&G has already implemented the controls to protect sensitive Bulk Electric System (BES) data while being transmitted over communications links between BES Control Centers.

Likes 0	
Dislikes 0	

Response

Rick Applegate - Tacoma Public Utilities (Tacoma, WA) - 6

Answer	No

Document Name	
Comment	

Tacoma Power endorses the draft comments shared with it by Salt River Project (SRP), which follow:

SRP does not agree the current standard and implementation plan can be executed in a cost effective manner. Encryption is the only solution available to protect both confidentiality and integrity for the data within this scope. If the implementation timeframe remains at 24 months, more resources and capital will be required versus a phased implementation. A phased implementation provides the ability to not only ensure the most effective plan, but also provides the ability to plan more accurately within budget cycles. More importantly, if encryption fails, SRP would lose Real-time Assessment and Real-time monitoring and control data. SRP is concerned a 24 month implementation timeline would impact reliability as there are many opportunities for encryption to fail that must be addressed. This has a direct correlation on cost when addressing those opportunities during this timeframe.

Likes 0	
Dislikes 0	
Response	
Oshani Pathirane - Oshani Pathirane On Behalf of: Payam Farahbakhsh, Hydro One Networks, Inc., 1, 3; - Oshani Pathirane	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	

As noted in earlier comments, clarification of the “control data” term is needed to fully assess our ability to address the standard in a cost effective manner. The flexibility built in to the current revision of R1 should support consideration of cost effective alternatives.

Likes 0	
Dislikes 0	
Response	

Richard Vine - California ISO - 2	
Answer	Yes
Document Name	
Comment	
The California ISO supports the comments of the IRC Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	
Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 3	
Answer	Yes
Document Name	
Comment	
PNMR believes the reliability objectives can be met in a cost effective manner for any internal links. However it is difficult to determine if links to external Entities can be met in a cost effective manner. PNMR agrees with AEP's concern of "mutually agreed upon: formats, processes for resolving conflicts and security protocols" can affect the cost of implementation. Yet PNMR currently does not see an instance where this would greatly impact the cost of implementation.	
Likes 0	
Dislikes 0	
Response	
Annette Johnston - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	Yes
Document Name	
Comment	
no comments	
Likes 0	
Dislikes 0	
Response	

Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
The proposed Standard, as written, provides entities flexibility on implementation.	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Infrastructure will have to be added, and the standard allows for flexibility. There are some concerts that data exchange with other entities may become difficult, and it may become costly to support that infrastructure.	
Likes 0	
Dislikes 0	
Response	
Laurie Williams - PNM Resources - Public Service Company of New Mexico - 1	
Answer	Yes
Document Name	
Comment	
PNMR believes the reliability objectives can be met in a cost effective manner for any internal links. However it is difficult to determine if links to external Entities can be met in a cost effective manner. PNMR agrees with AEP's concern of "mutually agreed upon: formats, processes for resolving conflicts and security protocols" can affect the cost of implementation. Yet PNMR currently does not see an instance where this would greatly impact the cost of implementation.	
Likes 0	
Dislikes 0	
Response	

sean erickson - Western Area Power Administration - 1	
Answer	Yes
Document Name	
Comment	
As noted in earlier comments, clarification of the “control data” term is needed to fully assess our ability to address the standard in a cost effective manner. The flexibility built in to the current revision of R1 should support consideration of cost effective alternatives.	
Likes 0	
Dislikes 0	
Response	
David Francis - SRC - 2 - MRO,Texas RE,NPCC,SERC,RF, Group Name SRC + SWG	
Answer	Yes
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	
Steven Powell - Trans Bay Cable LLC - NA - Not Applicable - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 3, Group Name FirstEnergy Corporation	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	
Likes 2	PSEG - Public Service Electric and Gas Co., 1, Smith Joseph; PSEG - Public Service Electric and Gas Co., 3, Mueller Jeffrey
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eleanor Ewry - Puget Sound Energy, Inc. - 5	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Chris Scanlon - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chantal Mazza - Hydro-Qu?bec TransEnergie - 2 - NPCC	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brandon McCormick - Brandon McCormick On Behalf of: Ginny Beigel, City of Vero Beach, 3; Lynne Mila, City of Clewiston, 4; Tom Reedy, Florida Municipal Power Pool, 6; - Brandon McCormick, Group Name FMPA	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb On Behalf of: Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; James McBee, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; Jessica Tucker, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; Jim Flucke, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; - Douglas Webb	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
larry brusseau - Corn Belt Power Cooperative - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ronald Donahey - TECO - Tampa Electric Co. - 3	
Answer	
Document Name	
Comment	
TEC wishes to endorse the comment of the Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	
W. Dwayne Preston - Austin Energy - 3	
Answer	
Document Name	
Comment	
I support Andrew Gallo's Comments from Austin Energy.	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	

Texas RE does not have comments on this question.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	
Document Name	
Comment	
Cost effectiveness will be determined by the Entity’s implementation and existing contracts.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion and ISO-NE	
Answer	
Document Name	
Comment	
Cost effectiveness will be determined by the Entity’s implementation and existing contracts.	
Likes 0	
Dislikes 0	
Response	

6. If you have additional comments on the proposed CIP-012-1 – Cyber Security – Communications between Control Centers drafted in response to the FERC directive that you have not provided in response to the questions above, please provide them here.

Rick Applegate - Tacoma Public Utilities (Tacoma, WA) - 6

Answer	
Document Name	

Comment

Thank you for your consideration.

Likes 0	
Dislikes 0	

Response

Brandon Cain - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - FRCC,MRO,WECC,Texas RE,SERC,SPP RE, Group Name Southern Company

Answer	
Document Name	

Comment

Overall, Southern Company is concerned that the scope of data is too broad and subject to interpretation during audits without direct ties to the IRO and TOP standards requiring identification of the subject data. The nature of the data in Control Center environments is such that its criticality often changes based on the current situation. Entities performing TOP and BA functions, in particular, receive data from a variety of entities, each with its own data provision capabilities. A variety of data formats and delivery mechanisms are accommodated, and not all data received is needed at all times. Groupings of data and how those groupings are defined is important. Without endorsed Technical Rationale and Implementation Guidance, development of an appropriate technical plan to address this requirement and support successful audits of it remain a concern.

Southern Company feels that 12 months is appropriate to develop a plan, but an additional 24 months beyond planning may be needed to implement a reliable technical solution. Given the need to perform a proper engineering study on network infrastructure to assess current state and adapt it to meet the new requirements, additional time is needed to assess how changes may impact system and network response (loading, latency, etc). It will also be necessary to review and / or establish contracts and memorandums of understanding to ensure that we continue to reliably receive the data we need and to deliver the data that others may need from us. Inherent in these studies and implementations are additional costs that may be impacted by budget cycles, as well as the costs attributable to resource constraints given the constant environment of standards changes currently. These factors prevent any realistic analysis at this time of the cost-effectiveness of such implementations.

Apart from those noted above, Southern Company does not have any additional specific objections to the CIP-012-1 requirements, the draft Technical Rationale, or the draft Implementation Guidance. It is important to note that the Proposed Reliability Standard currently does not have *endorsed* Technical Rationale and Implementation Guidance. Due to this, Southern Company currently supports (with comments) the Proposed Reliability Standard with the understanding that NERC's endorsement of the Implementation Guidance may impact our support for a final ballot of the standard.

Likes 0	
Dislikes 0	

Response

Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC

Answer	
Document Name	

Comment
There was a proposed revision to the definition of Control Center that was posted concurrently with the 1st posting of CIP-012-1. What is the status of that definition? Will both of these be Petitioned to FERC on the same filing? Could one get approved before the other?

Likes 0	
Dislikes 0	

Response

David Francis - SRC - 2 - MRO,Texas RE,NPCC,SERC,RF, Group Name SRC + SWG

Answer	
Document Name	

Comment
Comments: The SWG supports the objective-based requirements as written. The objective-based approach allows for Responsible Entities to select and implement the controls appropriate to their organization.

Likes 0	
Dislikes 0	

Response

Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric

Answer	
Document Name	

Comment
None at this time.

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion and ISO-NE	
Answer	
Document Name	
Comment	
Removal of the SDT's Guidance and Technical Basis (GTB) from the Standard makes it difficult to 1) understand the intent and 2) evaluate this version. If the GTB is not restored, we recommend posting the GTB information simultaneous with the Standard.	
Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	
Document Name	
Comment	
If the demarcation point for communication is a CIP Cyber Asset, communication of this information and responsibilities between entities for R1.2 may require NDAs between entities.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb On Behalf of: Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; James McBee, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; Jessica Tucker, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; Jim Flucke, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; - Douglas Webb	
Answer	
Document Name	
Comment	
None.	
Likes 0	
Dislikes 0	
Response	

Leonard Kula - Independent Electricity System Operator - 2	
Answer	
Document Name	
Comment	
Removal of the SDT's Guidance and Technical Basis (GTB) from the Standard makes it difficult to 1) understand the intent and 2) evaluate this version. If the GTB is not restored, we recommend posting the GTB information simultaneous with the Standard.	
Likes 0	
Dislikes 0	
Response	
David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	
Document Name	
Comment	
In the case of Medium and High Control Centers, if it is intended that communication be protected up to an EAP on the ESP and/or the PSP, then it is suggested that this demarcation point requirement should be clearly stated, possibly in an additional (sub-)requirement.	
Likes 0	
Dislikes 0	
Response	
Laurie Williams - PNM Resources - Public Service Company of New Mexico - 1	
Answer	
Document Name	
Comment	
While some entities have raised a concern that encryption or other security efforts could impact availability and thus nullify the FERC mandate regarding availability, PNMR does not believe that such security measure can have a significant detrimental effect on availability if such measures are properly designed and implemented. PNMR believes that this standard really addresses the Confidentiality and Integrity of sensitive BES data while TOP-001-4 addresses the Availability of such data between primary Control Centers. Thus the standards are better ensuring all aspects of the Confidentiality-Integrity-Availability triad are addresses in some way. All three aspects can be maintained in unison. Implementing processes and procedures to address one aspect does not implicitly result in the absence or detriment of the other two.	
Likes 0	

Dislikes 0	

Response

Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	
Document Name	

Comment
While EEI does not currently have any specific objections to CIP-012-1 Requirements, Implementation Plan or the flexibility to meet the reliability objectives in a cost-effective manner, we do note that the Proposed Reliability Standard lacks sufficient specificity (i.e., sufficient to stand on its own), without endorsed Technical Rationale and Implementation Guidance. Relative to the draft Implementation Guidance document, EEI notes that Industry will likely find it difficult to make any final judgements on the proposed Reliability Standard without the ERO Enterprise's endorsement of the draft Implementation Guidance. We trust that once the Proposed Reliability Standard gets closer to a final ballot, the ERO Enterprise will endorse the final draft of the Implementation Guidance in accordance with the Compliance Guidance Policy. In the event, that doesn't occur, the approval of this standard may be at risk.

Likes 0	
Dislikes 0	

Response

Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	
Document Name	

Comment
City Light would like to thank everyone for their efforts towards making this viable.

Likes 0	
Dislikes 0	

Response

Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	
Document Name	

Comment

Comments: The SWG supports the objective-based requirements as written. The objective-based approach allows for Responsible Entities to select and implement the controls appropriate to their organization.

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	
Document Name	

Comment

Texas RE appreciates the SDT's efforts to better clarify the data protection obligations by establishing a requirement to create "demarcation points" between Control Centers. In particular, Texas RE applauds the SDT's amendment to recognize that communications between "any" Control Center should be protected. However, while this injects clarity into the standard, it does not completely address Texas RE's fundamental concerns with the proposed CIP-012 Standard language.

As Texas RE noted previously, Texas RE remains concerned that the proposed CIP-012-1 Standard may result in confusion, particularly among Generation Operators with Control Centers subject to the standard regarding the scope of their compliance obligations or, alternatively, may inadvertently result in a significant reliability gap given the structure of the ERCOT market. In ERCOT, generators do not communicate directly with the regional Reliability Coordinator (ERCOT). Instead, generators are required to communicate through designated entities known as Qualified Scheduling Entities (QSEs). In many instances, these QSEs are third-party entities. Within the NERC regulatory construct, Generator Operators have delegated certain NERC compliance functions to these entities, including providing data used for Operational Planning Analysis, Real-time Assessments, and Real-time monitoring. Critically, Generator Operators remain responsible for all compliance obligations associated with QSE activities in the ERCOT region.

Texas RE continues to believe that CIP-012-1 must require Generator Operators possessing Control Centers to take steps to mitigate the risk of unauthorized data disclosures at every step along the communication chain between its Control Center and the ERCOT Control Center, including steps to protect this data at third-party intermediary QSEs. Otherwise, the proposed draft of CIP-012-1 would result in a significant reliability gap as QSE communications links and data passing from the QSE to ERCOT could be potentially unsecure. Given this fact, Generator Operators will likely need to take steps to ensure that their third-party QSEs have accorded designated sensitive data appropriate protections, which could in turn require incorporating such requirements into QSE agreements or other steps.

Permitting Generator Operators to merely designate a demarcation point potentially permits such entities to unduly restrict their compliance obligations. Generator Operators could set the demarcation point at their Control Center and the QSE. As a result, data and communication links between the QSE and the ERCOT Control Center could potentially be excluded from CIP-012 protections, resulting in a fundamental reliability gap.

Texas RE continues to recommend that the SDT clarify that communications between QSEs (or equivalent in other Regions) and the RC are subject to CIP-012-1 requirements and that Responsible Entities must take steps to address mitigate the risk of unauthorized data disclosures for these communications as well in order to ensure that Responsible Entities have sufficient notice of these compliance obligations.	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1	
Answer	
Document Name	
Comment	
While Exelon does not have any specific objections to CIP-012-1 Requirements, Implementation Plan or the flexibility to meet the reliability objectives in a cost-effective manner, we do note that the Proposed Reliability Standard lacks sufficient specificity (i.e., sufficient to stand on its own), without an endorsed Technical Rationale and Implementation Guidance. Relative to the draft Implementation Guidance document, Exelon notes that Industry will likely find it difficult to make any final judgments on the proposed Reliability Standard without NERC's endorsement of the draft Implementation Guidance. We trust that once the Proposed Reliability Standard gets closer to a final ballot NERC will endorse the final draft of the Implementation Guidance.	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	
Document Name	
Comment	
The VRF/VSL for proposed Requirement R2 should be revised to include a moderate and high VSL, similar to the proposed Requirement R1. Implementation of the plan, but failure to implement one of the applicable parts of the plan should be Moderate VSL. Implementation of the plan, but failure to implement two of the applicable parts should be High VSL. As stated in Response to Question No. 1, the proposed Standard should not move into final ballot until the definition of Control Center has been finalized.	
Likes 0	
Dislikes 0	
Response	

Annette Johnston - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	
Document Name	
Comment	
Support Terry Harbour comments (Berhshire Hathaway - MidAmerican Energy Company) We don't see the reason for two requirements. Implementation Guidance with approved ERO deference is essential for an affirmative ballot.	
Likes 0	
Dislikes 0	
Response	
Shannon Fair - Colorado Springs Utilities - 1,3,5,6	
Answer	
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Lona Calderon - Salt River Project - 1,3,5,6 - WECC	
Answer	
Document Name	
Comment	
SRP would like to thank the SDT for their efforts. This is an extremely difficult topic to handle and SRP appreciates all of the outreach the SDT has done.	
Likes 0	
Dislikes 0	

Response
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1
Answer	
Document Name	
Comment
The Proposed Reliability Standard lacks sufficient specificity (i.e., sufficient to stand on its own), without an endorsed Technical Rationale and Implementation Guidance. Relative to the draft Implementation Guidance document, MEC agrees with EEI that Industry will likely find it difficult to make any final judgments on the proposed Reliability Standard without NERC's endorsement of the draft Implementation Guidance. We trust that once the Proposed Reliability Standard gets closer to a final ballot NERC will endorse the final draft of the Implementation Guidance. In the event, that doesn't occur, we fear the approval of this standard may be at risk.
Likes 0	
Dislikes 0	
Response
W. Dwayne Preston - Austin Energy - 3
Answer	
Document Name	
Comment
I support Andrew Gallo's Comments from Austin Energy.
Likes 0	
Dislikes 0	
Response
Barry Lawson - National Rural Electric Cooperative Association - 4
Answer	
Document Name	
Comment
NRECA requests additional information on how the draft revised Control Center definition and the draft new CIP-12-1 will move forward after this comment period. We believe they should move forward together in any next steps in the standard development process. Currently, when reviewing the draft new CIP-12-1 it is unclear if the current approved Control Center definition or the draft revised Control Center definition is what the drafting team intends the reader to use.

NRECA appreciates the efforts of the drafting team.

Likes 0	
Dislikes 0	

Response

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group

Answer	
Document Name	

Comment

The SPP Standards Review Group proposes a few minor non-substantive edits to CIP-012-1 at Requirement R1 and Measurement M2. The edits will reference the term “plan(s)” and ensures consistent use of vernacular is used throughout the standard (see below for proposed language- in bold).

R1. The Responsible Entity shall develop one or more documented plan(s) to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring and control data while being transmitted between any Control Centers. This requirement excludes oral communications. The plan**(s)** shall include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M2. Evidence may include, but is not limited to, documentation demonstrating implementation of the plan**(s)** developed pursuant to Requirement R1.

Likes 0	
Dislikes 0	

Response

Nicholas Lauriat - Network and Security Technologies - 1

Answer	
Document Name	

Comment

(No additional comments)

Likes 0	
Dislikes 0	

Response

Eleanor Ewry - Puget Sound Energy, Inc. - 5

Answer	
Document Name	
Comment	

Please refer to EEI's comments regarding the Proposed Reliability Standard currently lacking sufficient specificity (i.e. sufficient to stand on its own) without an endorsed Technical Rationale and Implementation Guidance.

Likes 0	
Dislikes 0	
Response	

Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 3

Answer	
Document Name	
Comment	

While some entities have raised a concern that encryption or other security efforts could impact availability and thus nullify the FERC mandate regarding availability, PNMR does not believe that such security measure can have a significant detrimental effect on availability if such measures are properly designed and implemented. PNMR believes that this standard really addresses the Confidentiality and Integrity of sensitive BES data while TOP-001-4 addresses the Availability of such data between primary Control Centers. Thus the standards are better ensuring all aspects of the Confidentiality-Integrity-Availability triad are addresses in some way. All three aspects can be maintained in unison. Implementing processes and procedures to address one aspect does not implicitly result in the absence or detriment of the other two.

Likes 0	
Dislikes 0	
Response	

Andrew Gallo - Austin Energy - 6

Answer	
Document Name	
Comment	

AE thanks the SDT for their hard work on a difficult topic and appreciates the SDT's outreach efforts.

Likes 0	
Dislikes 0	
Response	

Vivian Vo - APS - Arizona Public Service Co. - 3	
Answer	
Document Name	
Comment	

The application of any security controls requires bilateral consent. The first priority of Requirement 1 should be to identify the methods through with the Responsible Entity determines and identifies these security controls and documentation the Responsible Entity intends to utilize throughout this identification/determination process. AZPS respectfully submits, for the SDT's consideration, the following revision of Requirement 1 to address the above-referenced comments.

Proposed Revision to CIP-012-1 R1:

R1.1 Identification of methods and documentation through which the Responsible Entity will determine and identify security controls used to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring and control data while being transmitted between Control Centers, and roles and responsibilities for implementation when the Control Centers are owned or operated by different Responsible Entities;

R1.2 Identification of security controls used to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring and control data while being transmitted between Control Centers; and

R1.3 Identification of demarcation point(s) where security controls is applied for transmitting Real-time Assessment and Real-time monitoring and control data between Control Centers.

Likes 0	
Dislikes 0	
Response	

Shelby Wade - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
Answer	
Document Name	
Comment	

PPL NERC Registered Affiliates supports EEI's comments regarding CIP-012-1 – Cyber Security – Communications between Control Centers: "*While EEI does not have any specific objections to CIP-012-1 Requirements, Implementation Plan or the flexibility to meet the reliability objectives in a cost effective manner, we do note that the Proposed Reliability Standard lacks sufficient specificity (i.e., sufficient to stand on its own), without an endorsed Technical Rationale and Implementation Guidance. Relative to the draft Implementation Guidance document, EEI notes that Industry will likely find it difficult to make any final judgements on the proposed Reliability Standard without the ERO Enterprise's endorsement of the draft Implementation Guidance. We trust that once the Proposed Reliability Standard gets closer to a final ballot, the ERO Enterprise will endorse the final draft of the Implementation Guidance in accordance with the Compliance Guidance Policy. In the event that doesn't occur, we fear the approval of this standard may be at risk.*"

Likes 0	
Dislikes 0	
Response	

Ronald Donahey - TECO - Tampa Electric Co. - 3	
Answer	
Document Name	
Comment	
TEC wishes to endorse the comment of the Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	
Document Name	
Comment	
The California ISO supports the comments of the IRC Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	
Paul Huettl - Basin Electric Power Cooperative - 6	
Answer	
Document Name	
Comment	
Please refer to NRECA comments.	
Likes 0	
Dislikes 0	
Response	
Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF	

Answer	
Document Name	
Comment	

Per R1.3, may create a level of difficulty where “each Responsible Entity” will need to know each other’s “roles and responsibilities … for applying security protection(s)”. The intent should be to assure that protections are in place and not create an administrative burden just to audit this. The use of the wording of “roles and responsibilities” does not support the cyber security protections that this Standard is trying to accomplish. Different responsible Entities may not be willing to share their “security protections” with other Entities as this may create a security gap or at the least, letting others know what protections are in place. When each Entity becomes compliant with this Standard, their plans will assure that protections are in place on “their end” of the data stream. This will assure that protections, which is the intent of this Standard.

The NSRF recommends R1.3 to read:

“Identify each Responsible Entity for applying security protection to the transmission of Real-time Assessment and Real-time monitoring and control data between Control Centers, when the Control Centers are owned or operated by different Responsible Entities”.

This recommendation will assure that each Responsible Entity will know who is on “the other end” of their data stream, which supports data security and intent of this Standard.

Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	
Document Name	
Comment	

None

Likes 0	
Dislikes 0	
Response	
Janis Weddle - Public Utility District No. 1 of Chelan County - 6, Group Name Chelan PUD	
Answer	
Document Name	
Comment	

Implementing industry-wide secure communication is a significant coordination challenge for entities and their associated vendors. The increase in security also brings increased complexity, maintenance, and failure potential that may negatively impact the reliable operation of the BES. As a result, coordination for encryption key management will become an essential activity and CHPD would, similar to other entity comments, appreciate guidance for these activities.

CHPD also has general concerns that implementing encryption results in the loss of existing application-level protocol security. For example, current security protections allow for the enforcement of specific ICCP protocol functions at the firewall perimeter. With end-to-end encryption in use (e.g., Secure ICCP) the firewall will no longer be able to inspect ICCP packets and will lose the ability to reject unauthorized commands (e.g., control, write, etc.).

Likes 5	Public Utility District No. 1 of Snohomish County, 5, Nietfeld Sam; Snohomish County PUD No. 1, 6, Lu Franklin; Public Utility District No. 1 of Snohomish County, 1, Duong Long; Snohomish County PUD No. 1, 3, Oens Mark; Public Utility District No. 1 of Snohomish County, 4, Martinsen John
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion

Answer	
Document Name	

Comment

The R1 VSL language does not accurately align with R1. Dominion Energy recommends adding the “develop” portion of R1 to the VSL language as shown in the following example.

“The Responsible Entity failed to develop and document plan(s) for Requirement R1.”

In addition, the rationale developed by the SDT does not appear to have been included in the document or moved to any type of reference document. The lack of any contextual documents creates a gap in understanding the intent of the SDT. Coupled with the lack of approved Implementation Guidance, it is difficult to support the Requirements as written.

Likes 0	
Dislikes 0	

Response

Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF

Answer	
Document Name	

Comment

N/A

Likes 0	
Dislikes 0	
Response	

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2016-01 Modifications to CIP Standards

Draft Reliability Standard Audit Worksheet (RSAW) Posted for Industry Comment through December 11, 2017

Now Available

The draft RSAW for **CIP-012-1 – Cyber Security – Control Center Communication Networks** is posted on the project page for industry comment through **8 p.m. Eastern, Monday, December 11, 2017.** Submit feedback regarding the draft RSAW to RSAWfeedback@nerc.net.

For more information or assistance, contact Katherine Street at (404) 446-9702 or Mat Bunch at (404) 446-9785.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Project 2016-02

Modifications to CIP Standards
Consideration of Comments to CIP-012-1
(Comment Period: October 27 – December 11, 2017)

March 2018

RELIABILITY | ACCOUNTABILITY



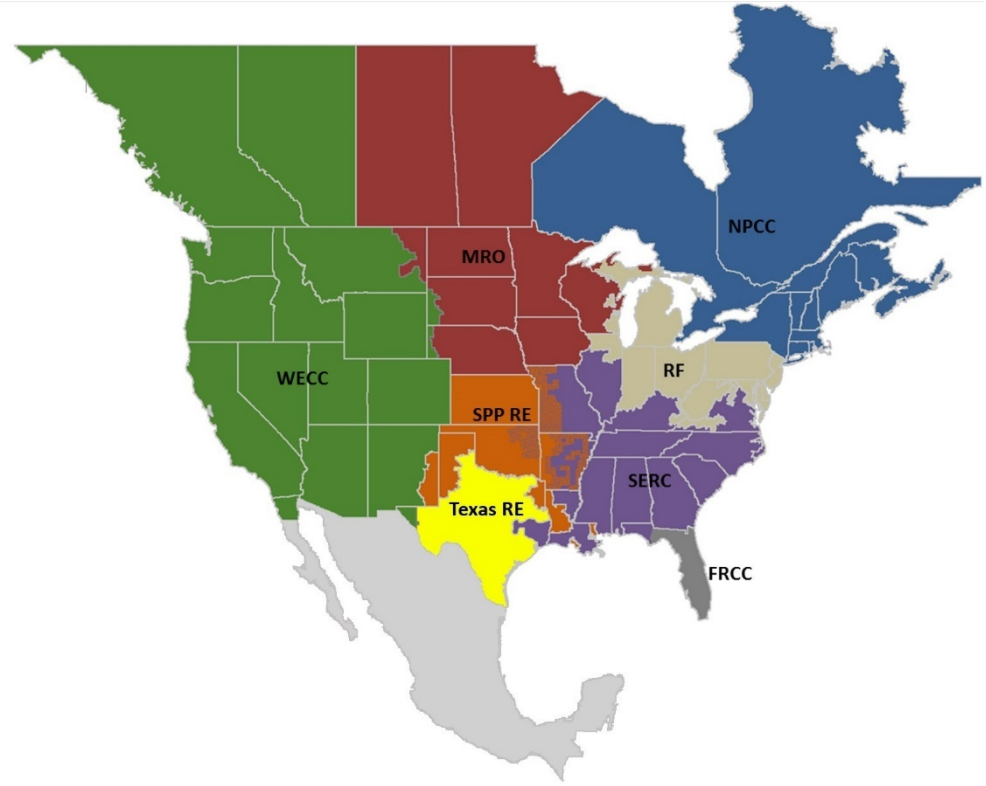

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Preface

The North American Electric Reliability Corporation (NERC) is a not-for-profit international regulatory authority whose mission is to assure the reliability and security of the bulk power system (BPS) in North America. NERC develops and enforces Reliability Standards; annually assesses seasonal and long-term reliability; monitors the BPS through system awareness; and educates, trains, and certifies industry personnel. NERC's area of responsibility spans the continental United States, Canada, and the northern portion of Baja California, Mexico. NERC is the Electric Reliability Organization (ERO) for North America, subject to oversight by the Federal Energy Regulatory Commission (FERC) and governmental authorities in Canada. NERC's jurisdiction includes users, owners, and operators of the BPS, which serves more than 334 million people.

The North American BPS is divided into eight Regional Entity (RE) boundaries as shown in the map and corresponding table below.



The North American BPS is divided into eight RE boundaries. The highlighted areas denote overlap as some load-serving entities participate in one Region while associated transmission owners/operators participate in another.

FRCC	Florida Reliability Coordinating Council
MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
SPP RE	Southwest Power Pool Regional Entity
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

The standard drafting team (SDT) appreciates industry comments on the proposed Reliability Standard, CIP-012. The SDT considered the comments submitted during the additional posting of the proposed Reliability Standard, and adapted its revision approach for the third proposal currently posted. Additionally, the SDT conducted substantial outreach during the revision process, through in-person meetings, conference calls, and stakeholder organization presentations.

On January 21, 2016, the Federal Energy Regulatory Commission (FERC) issued Order No. 822 Revised Critical Infrastructure Protection Reliability Standards. In this order, FERC approved revisions to version 5 of the CIP standards.

Response to Comments

The SDT has carefully reviewed each stakeholder comment and has revised language where suggested changes are consistent with SDT intent and industry consensus. The SDT reviewed and responded to each comment in summary form below.

There were 61 sets of comments comprised of approximately 168 different people across approximately 117 companies representing 10 of the Industry Segments.

All comments submitted can be reviewed in their original format on the project page.

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process. If you feel there has been an error or omission, you can contact the Senior Director of Standards, Howard Gugel (via email) or at (404) 446-9693.

Creation of CIP-012-1

- Multiple commenters noted that CIP-012 is not needed and can be accommodated within existing CIP Standards. The commenters also noted that encryption may not be feasible and the only remedy is to physically protect the entire communication system.

  The SDT contends that CIP-012 is needed as the application of protection is different for in-scope data while being transmitted between Control Centers than it is with other standards, such as CIP-005. CIP-012 addresses applicable data transmitted between Control Centers and backup Control Centers regardless of BES Cyber System impact rating. CIP-005 is applicable only to high and medium BES Cyber Systems. The SDT disagrees that the only way to achieve the security objective is to physically protect the entire communication system. Further, the SDT asserts that an entity can apply any combination of controls it sees fit to achieve the security objective. CIP-006 even acknowledges that physical protection may not be the only solution. Geographic distance is just one factor that needs to be evaluated that may preclude the use of physical protection alone.

- Several commenters provided support of CIP-012 and the requirements, noting the results-based approach allows Responsible Entities to select and implement the controls appropriate to their organization.

  The SDT thanks you for the comments.

- A commenter noted CIP-012 is not needed.

  The SDT contends that CIP-012 is needed. Applying protection for in-scope data while being transmitted between Control Centers in CIP-012 is different from applying data protection in other standards. CIP-012 is also applicable to all impact levels, unlike CIP-002 through CIP-011

- A commenter remains concerned that the proposed CIP-012 Standard may result in confusion, particularly among Generation Operators with Control Centers subject to the standard regarding the scope of their compliance obligations or, alternatively, may inadvertently result in a significant reliability gap given the structure of the ERCOT market. In ERCOT, generators do not communicate directly with the regional Reliability Coordinator (ERCOT). Instead, generators are required to communicate through designated entities known as Qualified Scheduling Entities (QSEs). In many instances, these QSEs are third-party entities. Within the NERC regulatory construct, Generator Operators have delegated certain NERC compliance functions to these entities, including providing data used for Operational Planning Analysis, Real-time Assessments, and Real-time monitoring. Critically, Generator Operators remain responsible for all compliance obligations associated with QSE activities in the ERCOT region.

  The Responsible Entity that delegates its functional responsibilities to a third party agent through a contract or otherwise, continues to be responsible for compliance with NERC Reliability Standards. CIP-012-1 is applicable to NERC-registered Generator Operators and Generator Owners. Responsible Entities are to ensure that Real-time Assessment and Real-time monitoring data is protected throughout the transmission between each Control Center, regardless of any other third party in the middle of the transmission of the data. To address the concerns with coordination between Responsible Entities, modified the requirement to include, "If the Control Centers are owned or operated by different Responsible Entities, identify the responsibilities of each Responsible Entity for applying security protection to the transmission of Real-time

Assessment and Real-time monitoring data between those Control Centers". This requires entities to participate in this coordination while maintaining flexibility on implementation of this requirement.

Requirement 1

- A commenter requested that the requirement be modified to require each Responsible Entity to mitigate the risk of unauthorized disclosure or modification of its own BES data between its own Control Centers.

  FERC Order 822 specifically notes that the protection of sensitive BES data transmitted between Control Centers should be implemented for both inter- and intra-entity transmissions of data. The SDT developed CIP-012 in response to the FERC Order.

- A commenter recommended a change in the order of the three sub-requirements in Requirement R1.

  The SDT has identified the required actions to be taken within Requirement R1. During SDT discussions, entities varied on which step they would complete first. The requirement parts can be completed in any order. Requirement R1.3 is listed last since it may not be applicable to all entities

- A commenter proposed a few minor non-substantive edits to CIP-012 Requirement R1 and Measurement M2. The edits reference the term "plan(s)" and ensures consistent use throughout the standard

  The SDT has modified Requirement R1 as noted and has combined Requirements R1 and R2.

- Commenters noted concerns regarding the resolution of disagreements under Requirement R1.3.

  The SDT asserts that it is every Responsible Entity's obligation as defined in CIP-012, to protect data while being transmitted between Control Centers. The SDT cannot comment on specific approaches to resolve conflicts that arise in defining responsibilities between entities. Entities should consider working with the Regional Entity where there are unresolved disagreements.

- A commenter noted it is not clear how Requirement R1 addresses future Control Centers since the requirement suggests a one-time plan.

  The SDT asserts that Requirement R1 is not intended to be a one-time plan. A Responsible Entity will need to produce a plan to protect all in-scope data while being transmitted between Control Centers. This plan will need to apply to all Control Centers that a given entity owns or operates. As the number of Control Centers within an entity's purview changes, so should the plan and implementation of the plan be changed.

- A commenter noted that the requirement should specify creation of a documented process instead of a documented plan.

  The SDT disagrees regarding the use of the term "process" instead of "plan," the SDT notes that the term 'documented process' refers to a set of required instructions specific to the Responsible Entity developed to achieve a specific outcome. The plan to meet Requirement R1 may simply be a documentation of the architecture in place to provide the defined security protection and not a series of instructions or steps to be followed.

Requirement 2

- Commenters requested that the SDT consider consolidating Requirement R2 into Requirement R1, noting it is unnecessary to have two requirements. The commenters also noted that the requirement should specify creation of a documented process instead of a documented plan.

  The SDT agrees with comments regarding a single requirement and has modified Requirement R1 accordingly. With regard to the use of the term "process" instead of "plan", the SDT notes that the term documented process refers to a set of required instructions specific to the Responsible Entity, designed to achieve a specific outcome. The plan to meet Requirement R1 may simply be a documentation of the architecture in place to provide the defined security protection and not a series of instructions or steps to be followed.

- Commenters requested that the SDT consider consolidating Requirement R2 into Requirement R1, noting it is unnecessary to have two requirements.

  The SDT agrees with comments regarding a single requirement and has modified Requirement R1 accordingly.

Identification of Data

- A commenter requested that CIP-012-1 or supporting documents explicitly state that market data is out of scope.

  The SDT asserts that the data a Balancing Authority requires to perform Real-time monitoring and Real-time Assessments is the appropriate data to be protected under CIP-012-1. Where there is information being requested by a Balancing Authority or other Responsible Entity performing Real-time monitoring and Real-time Assessments, the SDT advises coordination between the Responsible Entities to ensure the correct data is identified and protected accordingly.

- Multiple commenters noted that all data elements should be evaluated in their unique context and that confidentiality protection is not needed for all data.

  The SDT has established the security objective in Requirement R1 to address the Commission's directive on protecting the confidentiality (unauthorized disclosure) and integrity (unauthorized modification) of the data being transmitted. The SDT asserts that data used for Real-time monitoring and Real-time Assessment is critical to the reliable operation of the Bulk Electric System and needs to be protected from unauthorized disclosure and modification. The SDT determined it would be a complex and difficult exercise for an Entity to define the protection required for various data elements in every situation. Therefore, the SDT chose to high water mark all of the in-scope data. In addition, the SDT notes that most, if not all of the methods applied to protect the integrity of data also inherently protect the confidentiality of the data.

- Commenters noted that viewing Real-time Assessment and monitoring/control data without context will adversely affect reliable operation of the BES and believes not all in-scope data requires the same level of confidentiality.

  The SDT has established the security objective in Requirement R1 to address the Commission's directive on protecting the confidentiality (unauthorized disclosure) and integrity (unauthorized modification) of the data being transmitted. The SDT asserts that data used for Real-time monitoring and Real-time Assessment is critical to the reliable operation of the Bulk Electric System, and thus needs to be protected from unauthorized disclosure and modification. The SDT determined it be a complex and difficult exercise

for an Entity to define the protection required for various data elements in every situation. Therefore, the SDT chose to high water mark all of the in-scope data. The SDT also notes that most, if not all, of the methods applied to protect the integrity of data also inherently protect the confidentiality of data.

- A commenter is concerned that the scope of data is too broad and subject to interpretation during audits without direct ties to the IRO and TOP standards requiring identification of the subject data.

The SDT discussed referencing the two applicable standards in the requirement language and determined that a number of issues could arise by directly referencing applicable IRO/TOP requirements. Possible issues include, but are not limited to, applicability issues and the required coordination of future revisions of the IRO/TOP standards and proposed Reliability Standard CIP-012.

Control Data

- Multiple commenters noted concerns with the meaning of "control data," noting it may create confusion and does not align with TOP-003 and IRO-010 data specification requirement.

The SDT agrees with the comments and has removed "and control" from Requirement R1.

Data Centers

- One commenter noted a concern with the definition of Control Center including associated data centers, specifically noting aggregating devices such as a dual port RTU could be interpreted as an associated data center to a Control Center.

As shown in the reference models and noted in the applicability section, communication between Control Centers and field devices, such as RTUs, are not in scope for CIP-012. The in-scope communications considered in CIP-012-1 are between two Control Centers, as defined in the NERC Glossary of Terms Used in Reliability Standards. Additionally, a data center not associated with the Control Center would be out of scope of CIP-012-1.

- A commenter noted that the communication link between Control Centers is in scope for CIP-012, but the link between Control Center and Data Center is not.

The SDT agrees that a Responsible Entity needs to protect the in-scope data while being transmitted between Control Centers. The SDT notes that the Control Center by definition includes the associated data center and should, therefore be included with protecting intra-Control Center communications. The SDT envisions a scenario where intra-Control Center communications not afforded protection elsewhere in the Reliability Standards would need to be protected under CIP-012 R1.

Administrative Burden

- A commenter noted that defining "roles and responsibilities" may create an administrative burden. They noted that different Responsible Entities may not be willing to share their "security protections" with other entities as this may create a security gap or at the least, letting others know what protections are in place. When each Entity becomes compliant with this Standard, their plans will assure that protections are in place on "their end" of the data stream. This will assure that protections, which is the intent of this Standard.

The SDT developed Requirement R1.3 to only apply to situations where multiple entities are involved in the transmission of the applicable data. Those entities must have an agreement on security protection in order for the transmission to actually happen. The intent is for the entities to agree upon and document who is

responsible for the various aspects of the protection. It may not be practical for both entities to try to control encryption keys, etc.

VSL Language

- Commenters noted concerns with the VSLs for the requirements. First, the VSL for Requirement R2 should be revised to include a moderate and high VSL. Second, it was recommended to add "develop" to the VSL language for Requirement R1.

The SDT combined Requirement R2 into Requirement R1 and revised the VSLs. The SDT removed "develop" from the language of Requirement R1.

Defining Other Terms

- Commenters requested that the SDT define Real-time monitoring.

The SDT asserts that Real-time monitoring is a well understood concept that is included in the TOP and IRO standards.

- Commenters noted that viewing Real-time Assessment and monitoring/control data without context will adversely affect reliable operation of the BES and believes not all in-scope data requires the same level of confidentiality.

The SDT has established the security objective in Requirement R1 to address the Commission's directive on protecting the confidentiality (unauthorized disclosure) and integrity (unauthorized modification) of the data being transmitted. The SDT asserts that data used for Real-time monitoring and Real-time Assessment is critical to the reliable operation of the Bulk Electric System, and thus needs to be protected from unauthorized disclosure and modification. The SDT determined it be a complex and difficult exercise for an Entity to define the protection required for various data elements in every situation. Therefore, the SDT chose to high water mark all of the in-scope data. The SDT also notes that most, if not all, of the methods applied to protect the integrity of data also inherently protect the confidentiality of data.

Alignment to TOP-003 and IRO-010

- Commenters requested the SDT add functional registrations noted in TOP and IRO standards to CIP-012 in order to draw a more clear line to Entities responsible for defining the Real-time Assessment and Real-time monitoring data under TOP-003 and IRO-010.

The SDT agrees with the comments and supports that this provides clarity and prevents all entities subject to CIP-012-1 from creating their own identification of Real-time Assessment and Real-time monitoring data. The SDT has modified Requirement R1 to address this recommendation.

- Commenters noted that the types of data to be within scope, as identified by data specification lists originating from Requirements TOP-003 and IRO-010 are not specific enough to determine or limit the types of data, or communication methods that would need to be protected the data. These lists contain data and methods of communicating data that may not be considered relevant to the scope of CIP-012.

The SDT agrees and has removed "and control" from Requirement R1. The SDT asserts that the data listed in the data specifications required to perform Real-time monitoring and Real-time Assessments is the appropriate data to be protected under CIP-012-1. Where there are concerns with information being requested by another Responsible Entity performing Real-time monitoring and Real-time Assessments,

coordination between the Responsible Entities is advised to ensure the correct data is identified and protected accordingly.

Third Parties

- Commenters noted that the guidance regarding third parties involved in the communication of Real-time Assessment and Real-time monitoring data is unclear. Further, some Generator Owners and Generator Operators neither own nor operate Control Centers due to agency relationships or through contracts with companies that are not NERC registered entities.

  The SDT agrees with the comments regarding the guidance on third parties and has removed the content. The Responsible Entity that delegates its functional responsibilities to a third party agent through a contract or otherwise, continues to be responsible for compliance with NERC Reliability Standards.

Demarcation Point

- Commenters noted that the demarcation point should be constrained to entity's equipment and not include an implied requirement that each entity document both their demarcation points and the demarcation points on neighboring systems.

  The SDT agrees and has modified the draft requirement accordingly.

- Commenters noted the importance of clarifying that demarcation points do not add additional Cyber Assets to the scope of the CIP standards CIP-002 through CIP-011.

  The SDT does not intend for CIP-012 to modify the list of Cyber Assets managed under CIP-002 thru CIP-011. This has been addressed within the Technical Rationale and Justification for Reliability Standard CIP-012-1.

Implementation

- A majority of commenters indicated that twenty-four months is an adequate standard implementation timeline. It allows entities sufficient time to develop internal plans to implement the enhanced security requirements. It also provides time to negotiate the necessary security changes between entities, and to make appropriate contract adjustments with service providers.

  The SDT thanks you for your comments.

- A commenter noted that the CIP-012 implementation period seems to be an excessively long to implement this proposed standard since security of real-time data is important and should be prioritized.

  The SDT determined that the complexity of the implementation needed an allowance of up to twenty-four (24) months for implementation. Entities have the flexibility to phase in their implementation of the requirement as long as all activities are completed within 24 months.

- Several commenters noted that more time is needed for implementation of CIP-012. Reasons included coordination with other entities, as well as specification, design, budgeting, implementation, and testing. Commenters also raised concerns on the impact to existing contractual agreements.

  The SDT carefully considered all comments and concluded that many factors should be considered to determine an implementation period. These factors include complexity of technology solutions, quantity of

telecommunications lines requiring controls and coordination with other Responsible Entities/solution providers. The SDT concluded that a twenty-four (24) month implementation period is appropriate.

- A commenter feels that 12 months is appropriate to develop a plan, but an additional 24 months beyond planning may be needed to implement a reliable technical solution. Given the need to perform a proper engineering study on network infrastructure to assess current state and adapt it to meet the new requirements, additional time is needed to assess how changes may impact system and network response (loading, latency, etc.). It will also be necessary to review and / or establish contracts and memorandums of understanding to ensure that we continue to reliably receive the data we need and to deliver the data that others may need from us. Inherent in these studies and implementations are additional costs that may be impacted by budget cycles, as well as the costs attributable to resource constraints given the constant environment of standards changes currently. These factors prevent any realistic analysis at this time of the cost-effectiveness of such implementations.

  The SDT carefully considered all comments and concluded that many factors should be considered to determine an implementation period. These factors include complexity of technology solutions, quantity of telecommunications lines requiring controls and coordination with other Responsible Entities/solution providers. The SDT concluded that a twenty-four (24) month implementation period is appropriate. Entities have the flexibility to phase in their implementation of the requirement as long as all activities are completed within 24 months.

Cost Effectiveness

- Several commenters noted they were unable to address the issue of cost effectiveness in full at this time. They noted the cost of implementation could not be adequately assessed until discussion and coordination with our neighboring entities. Cost effectiveness of implementation will depend on the technology deployed. Infrastructure may need to be added to support the requirement and may be costly to contract and support.

  The SDT carefully considered all comments and concluded that many factors should be considered to determine an implementation period. These factors include complexity of technology solutions, quantity of telecommunications lines requiring controls and coordination with other Responsible Entities/solution providers. CIP-012 has been written to allow entities flexibility in determining the solutions that work best for the organization and those they share this information with.

- Several commenters noted the need for an encryption standard to be developed across the various regions. The implementation of several different technologies to communicate with several different Reliability Coordinators and utilities would be overly burdensome and at a cost that would not be effective. It was noted that there is little that is mutually agreed upon in the data specification documents as they relate to IRO-010 and TOP-003. The Balancing Authority, Transmission Operator, and Reliability Coordinator specify the data they want to receive in the manner they want to receive it. Others receiving the requests are obligated to comply. Additionally, a commenter noted that the lack of guidance could lead to inconsistency of implementation.

  The SDT agrees a common standard would be highly beneficial to those operating in multiple regions. The SDT will refer the issue to the CIPC for review and consideration as a guideline.

- Several commenters noted the proposal cannot be implemented in a cost-effective manner within twenty-four (24) months. If the implementation period remains 24 months, entities will expend more resources and capital than using a phased implementation. A phased implementation provides the ability to ensure the most effective plan and plan more accurately within budget cycles. Commenters noted a 24-month

implementation timeline could affect reliability because many opportunities exist for encryption to fail and those challenges must be addressed, which has a direct effect on cost.

The SDT carefully considered all comments and concluded that many factors should be considered to determine an implementation period. These factors include complexity of technology solutions, quantity of telecommunications lines requiring controls and coordination with other Responsible Entities/solution providers. The SDT concluded that a twenty-four (24) month implementation period is appropriate. Entities have the flexibility to phase in their implementation of the requirement as long as all activities are completed within 24 months.

- One commenter recommended development of an exception process can be defined if needed to offer flexibility.

In order to evaluate this request, the SDT needs additional information and invites the commenter to participate in the regularly scheduled meetings.

Guideline and Technical Basis / Rationale

- Several commenters raised concerns with the lack of a Guidelines and Technical Basis (GTB) section of CIP-012. They noted the lack of GTB makes it difficult to understand the drafting team's intent, and evaluate the standard.

The SDT developed and posted Technical Rationale and Implementation Guidance documents to support CIP-012. The SDT will submit the Implementation Guidance for ERO endorsement once the requirement language is finalized.

- Several commenters discussed the criticality of having the Technical Rationale completed and Implementation Guidance endorsed for CIP-012. They noted industry will likely find it difficult to make any final judgments on the proposed Reliability Standard without NERC's endorsement of the draft Implementation Guidance. In the event the Implementation Guidance is not endorsed, there are fears the approval of this standard may be at risk.

The SDT developed and posted Technical Rationale and Implementation Guidance documents to support CIP-012. The SDT will submit the Implementation Guidance for ERO endorsement once the requirement language is finalized.

- Another commenter requested that the SDT provide a rationale for including the phrase "CIP Exceptional Circumstances." The same commenter further stated that it is particularly unclear why certain CIP exception conditions necessarily trigger CIP Exceptional Circumstances events. For example, why would an imminent hardware failure under all circumstances require a relaxation of physical security protection for communications links transmitting sensitive data?

The SDT drafted the requirement with the understanding that there may be instances where a Responsible Entity may not be able to maintain compliance with the requirement because of a CIP Exceptional Circumstance. Responsible Entities may need to use alternate, as-yet-unidentified data transmission methods because of a CIP Exceptional Circumstance event. This allowance will enable Responsible Entities to focus on reliability without the risk of a compliance issue.

Control Center Definition

- Commenters raised questions on the prior proposal for modifying the definition of Control Center. The commenters noted modifications to the definition and CIP-012 should move forward together in future steps in the standard development process. They also noted that when reviewing the new current draft of CIP-012, it is unclear if the current approved Control Center definition or the draft revised Control Center definition is what the drafting team intends the reader to use.

  The SDT has developed and posted modifications to the Control Center definition.

Medium / High Impact Control Centers

- Commenters questioned in the case of medium and high impact Control Centers, whether it is intended for the communication to be protected up to an Electronic Access Point on the Electronic Security Perimeter and/or the Physical Security Perimeter. If that is the intent, it is suggested that the demarcation point requirement clearly state this. It was also noted that if the demarcation point for communication is a CIP Cyber Asset, communication of this information and responsibilities between entities may require NDAs between entities.

  The SDT does not intend for CIP-012 to prescribe the point where security protection is applied. Depending on the entity, it may be at an ESP or it may not. It is the point where the protection can be applied before it is transmitted to another Control Center. The same consideration should be made in determining the physical protection. The SDT agrees that proper care should be taken with sharing information that could be considered BES Cyber System Information.

CIP-012 Applicability

- A commenter requested clarification on which Control Centers are applicable under CIP-012.

  The SDT drafted CIP-012 to apply to all types of Control Centers, regardless of the impact rating associated with the Control Centers' BES Cyber Systems.

- A commenter noted that Generator Owners are not listed in the Control Center definition and should be removed from applicability of CIP-012.

  The SDT modified the applicability of the Standard as, "The requirements in this standard apply to the following functional entities, referred to as "Responsible Entities," that own or operate a Control Center." The SDT intends for the standard to include Generator Owners and Transmission Owners that own or operate a Control Center. The Control Center definition as written addresses the reliability tasks of an RC, BA, TOP, and GOP irrespective of registration. The SDT has developed and posted modifications to the Control Center definition.

Compliance

- A commenter requested clarification on the responsibility for compliance, including who will be audited under CIP-012.

  The SDT asserts that entities that own and/or operate Control Centers, per Section 4 "Applicability" are responsible to document and implement a plan to protect the data specified in CIP-012. The Responsible Entity that delegates its functional responsibilities to a third party agent through a contract or otherwise, continues to be responsible for compliance with NERC Reliability Standards.

FERC Directive 822

- A commenter noted it would be more effective if the SDT specifically identified the security objective described in FERC Order No. 822 paragraph 54, of "maintaining the integrity and availability of sensitive BES data", should account for risk of cyber assets, and should be results based and not zero-defect.

  The SDT asserts that the security objective is clear and aligns with FERC Order 822, taking into consideration the sensitivity of the data being transmitted. As drafted, the development and implementation of a plan allows entities to tailor protection to their environment.

DRAFT

Cyber Security – Communications Between Control Centers

Technical Rationale and Justification for Reliability Standard CIP-012-1

November 2017

Table of Contents

Introduction

On January 21, 2016, the Federal Energy Regulatory Commission (FERC or Commission) issued Order No. 822, approving seven Critical Infrastructure Protection (CIP) Reliability Standards and new or modified terms in the Glossary of Terms Used in NERC Reliability Standards, and directing modifications to the CIP Reliability Standards. Among others, the Commission directed the North American Electric Reliability Corporation (NERC) to "develop modifications to the CIP Reliability Standards to require Responsible Entities[1] to implement controls to protect, at a minimum, communication links and sensitive bulk electric system data communicated between bulk electric system Control Centers in a manner that is appropriately tailored to address the risks posed to the bulk electric system by the assets being protected (i.e., high, medium, or low impact)." (Order 822, Paragraph 53)

In response to the directive in Order No. 822, the Project 2016-02 standard drafting team (SDT) drafted Reliability Standard CIP-012-1 to require Responsible Entities to implement controls to protect sensitive Bulk Electric System (BES) data and communications links between BES Control Centers. Due to the sensitivity of the data being communicated between Control Centers, as defined in the Glossary of Terms Used in NERC Reliability Standards, the standard applies to all impact levels (i.e., high, medium, or low impact).

Although the Commission directed NERC to develop modifications to CIP-006, the SDT determined that modifications to CIP-006 would not be appropriate. There are differences between the plan(s) required to be developed and implemented for CIP-012-1 and the protection required in CIP-006-6 Requirement R1 Part 1.10. CIP-012-1 Requirements R1 and R2 protect the applicable data during transmission between two separate Control Centers. CIP-006 Requirement R1 Part 1.10 protects nonprogrammable communication components within an Electronic Security Perimeter (ESP) but outside of a Physical Security Perimeter (PSP). The transmission of applicable data between Control Centers takes place outside of an ESP. Therefore, the protection contained in CIP-006-6 Requirement R1 Part 1.10 does not apply.

The SDT drafted requirements to provide Responsible Entities the latitude to protect the communication links, the data, or both, to satisfy the security objective consistent with the capabilities of the Responsible Entity's operational environment. Requirement R1 requires Responsible Entities to document one or more plans that protect Real-time Assessment and Real-time monitoring and control data while being transmitted between Control Centers. The plan(s) must address how the Responsible Entity will mitigate the risk of unauthorized disclosure or modification of the applicable data. Requirement R2 covers implementation of the plan developed according to Requirement R1.

This technical rationale and justification document explains the technical rationale for the proposed Reliability Standard. It will provide stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. It also contains information on the SDT's intent in drafting the requirements.

[1] As used in the CIP Standards, a Responsible Entity refers to the registered entities subject to the CIP Standards.

Requirement R1

R1. The Responsible Entity shall develop one or more documented plan(s) to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring and control data while being transmitted between any Control Centers. This requirement excludes oral communications. The plan shall include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1 Identification of security protection used to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring and control data while being transmitted between Control Centers;

1.2 Identification of demarcation point(s) where security protection is applied for transmitting Real-time Assessment and Real-time monitoring and control data between Control Centers; and

1.3 Identification of roles and responsibilities of each Responsible Entity for applying security protection to the transmission of Real-time Assessment and Real-time monitoring and control data between Control Centers, when the Control Centers are owned or operated by different Responsible Entities.

General Considerations for Requirement R1

Requirement R1 focuses on developing a plan to protect information that is critical to the real-time operations of the Bulk Electric System while in transit between applicable Control Centers.

Overview of confidentiality and integrity

The SDT drafted CIP-012-1 to address confidentiality and integrity of Real-time Assessment and Real-time monitoring and control data. This is accomplished by drafting the requirement to mitigate the risk of unauthorized disclosure (confidentiality) or modification (integrity). For this Standard, the SDT relied on the definitions of confidentiality and integrity as defined by National Institute of Standards and Technology (NIST):

- Confidentiality is defined as, "Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information."[2]
- Integrity is defined as, "Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity."[3]

The SDT asserts that the availability of this data is already required by the performance obligation of the Operating and Planning Reliability Standards. The SDT drafted CIP-012 to address the data while being transmitted. The SDT maintains that this data resides within BES Cyber Systems, and while at rest is protected by CIP-003 through CIP-011.

Alignment with IRO and TOP standards

The SDT recognized the FERC reference to additional Reliability Standards and the responsibilities to protect the applicable data in accordance with NERC Reliability Standards TOP-003 and IRO-010. The SDT used these references to drive the identification of sensitive BES data and chose to base the CIP-012 requirements on the Real-time data specification elements in these standards. This approach provides consistent scoping of identified data, and does not require each entity to devise its own list or inventory of this data. Many entities are required to provide this data under agreements executed with their RC, BA or TOP, often without benefit of knowing how those entities use that data.

[2] NIST Special Publication 800-53A, Revision 4, page B-3

[3] NIST Special Publication 800-53A, Revision 4, page B-6

The SDT notes that it expanded the phrase “Real-time monitoring” data from TOP-003 and IRO-010 to “Real-time monitoring and control” data. The SDT was concerned that data transmitted between Control Centers that results in the physical operation of BES Elements was not explicitly included in Real-time monitoring data. The SDT understands that in practice Real-time control data is not transmitted separately from Real-time monitoring data. However, the SDT wanted to ensure that Real-time control data was included regardless of whether or not it is transmitted along with Real-time monitoring data. If entities only transmit Real-time control data along with Real-time monitoring data, then the SDT does not intend for such entities to identify additional data beyond that Real-time monitoring data already included in the data specifications for TOP-003 and IRO-010.

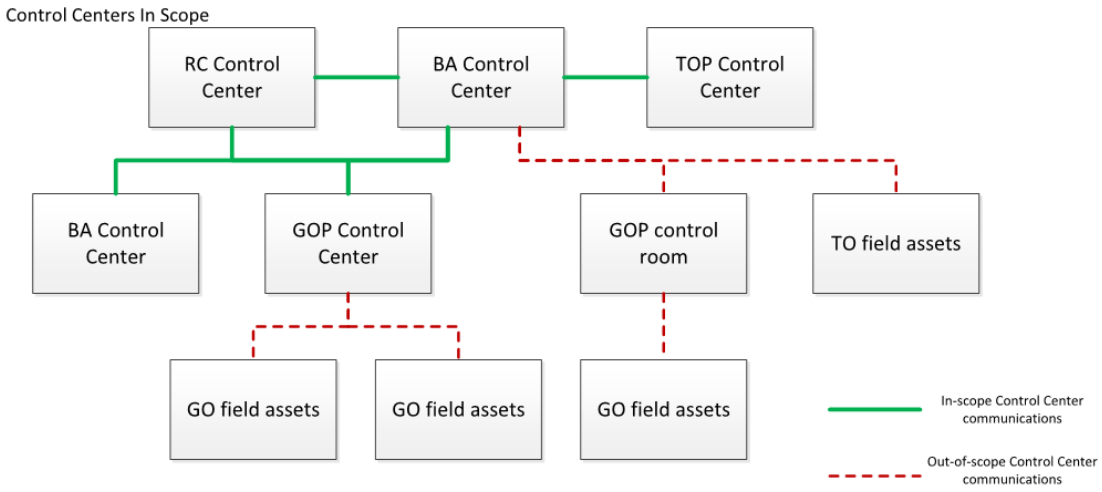
Demarcation Points

The SDT noted the need for an entity to identify a demarcation point inside each Control Center where it will apply protection for applicable data. The SDT used the demarcation point concept for implementing protection to ensure entities could still take advantage of security measures, such as deep packet inspection, already implemented at or near the EAP when ESPs are present, while maintaining the capability to protect the applicable data being transmitted between Control Centers.

Control Center Ownership

The requirements address protection for Real-time Assessment and Real-time monitoring and control data while being transmitted between Control Centers owned by a single Responsible Entity. They also cover the applicable data transmitted between Control Centers owned by two or more separate Responsible Entities. Unlike protection between a single Responsible Entity’s Control Centers, applying protection between Control Centers owned by more than one Responsible Entity requires additional coordination. The requirements do not explicitly require formal agreements between Responsible Entities partnering for protection of applicable data. It is strongly recommended, however, that these partnering entities develop agreements, or use existing ones, to define responsibilities to ensure adequate protection is applied. An example noted in FERC Order No. 822 Paragraph 59 is, “if several registered entities have joint responsibility for a cryptographic key management system used between their respective Control Centers, they should have the prerogative to come to a consensus on which organization administers that particular key management system."

As an example, the reference model below depicts some of the data transmissions between Control Centers that a Responsible Entity should consider to be in-scope. The example does not include all possible scenarios. The green solid lines are in-scope communications. The red dashed lines are out-of-scope communications.



This reference model is an example and does not include all possible scenarios.

Requirement R2

R2. The Responsible Entity shall implement the plan(s) specified in Requirement R1, except under CIP Exceptional Circumstances.

General Considerations for R2

Responsible Entities can achieve the security objective of Requirement R1 through a variety of methods or combinations of methods, such as site to site encryption, application layer encryption, physical protection, etc. The protection must be designed to prevent unauthorized disclosure or modification of applicable data on the applicable communication methods between Control Centers identified in Requirement R1.1. The Responsible Entity has the discretion to implement any type of protection that meets the security objective.

References

Here are several references to assist entities in developing plan(s) for protection of communication links:

- NIST Special Publication 800-53A, Revision 4: Security and Privacy Controls for Federal Information Systems and Organizations
- NIST Special Publication 800-82: Guide to Industrial Control Systems (ICS) Security
- NIST Special Publication 800-175B: Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms
- NIST Special Publication 800-47: Security Guide for Interconnecting Information Technology Systems

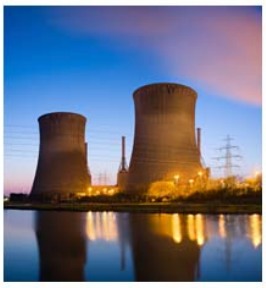
NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DRAFT

Cyber Security – Communications Between Control Centers

Implementation Guidance for CIP-012-1

RELIABILITY | ACCOUNTABILITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents




3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Introduction

The Commission issued Order No. 822 on January 21, 2016. Order 822 approved seven CIP Reliability Standards and new or modified definitions, and directed modifications be made to the CIP Reliability Standards. Among other items, the Commission directed NERC to "develop modifications to the CIP Reliability Standards to require responsible entities to implement controls to protect, at a minimum, communication links and sensitive bulk electric system data communicated between bulk electric system Control Centers in a manner that is appropriately tailored to address the risks posed to the bulk electric system by the assets being protected (i.e., high, medium, or low impact)." (Order 822, Paragraph 53)

In response to the directive in Order No. 822, the Project 2016-02 standard drafting team (SDT) drafted Reliability Standard CIP-012-1 to require Responsible Entities to implement controls to protect sensitive Bulk Electric System (BES) data and communications links between BES Control Centers. Due to the sensitivity of the data being communicated between Control Centers, the standard applies to all impact levels (i.e., high, medium, or low impact).

The SDT drafted requirements to provide Responsible Entities the latitude to protect the communication links, the data, or both, to satisfy the security objective consistent with the capabilities of the Responsible Entity's operational environment. Requirement R1 requires Responsible Entities to document one or more plans that protect Real-time Assessment and Real-time monitoring and control data while being transmitted between Control Centers. The plan(s) must address how the Responsible Entity will mitigate the risk of unauthorized disclosure or modification of the applicable data. Requirement R2 covers implementation of the plan developed according to Requirement R1.

The Project 2016-02 SDT also drafted this Implementation Guidance document to provide examples of approaches to comply with CIP-012-1. Implementation Guidance does not prescribe the only approach, but is intended to highlight one or more approaches that would be effective ways to be compliant with the standard. As Implementation Guidance is only meant to provide examples, entities may choose alternative approaches that better fit their situation[1].

Responsible Entities may find it useful to consider this Implementation Guidance document along with the additional context and background provided in the SDT developed Technical Rationale and Justification for CIP-012-1 document.

[1] NERC's Compliance Guidance Policy

Requirements

R1. *The Responsible Entity shall develop one or more documented plan(s) to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring and control data while being transmitted between any Control Centers. This requirement excludes oral communications. The plan shall include: [Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. Identification of security protection used to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring and control data while being transmitted between Control Centers;

1.2. Identification of demarcation point(s) where security protection is applied for transmitting Real-time Assessment and Real-time monitoring and control data between Control Centers; and

1.3. Identification of roles and responsibilities of each Responsible Entity for applying security protection to the transmission of Real-time Assessment and Real-time monitoring and control data between Control Centers, when the Control Centers are owned or operated by different Responsible Entities.

R2. *The Responsible Entity shall implement the plan(s) specified in Requirement R1, except under CIP Exceptional Circumstances.*

General Considerations

General Considerations for R1

As noted in the Technical Rationale and Justification for CIP-012-1, the focus of Requirement R1 is on developing a plan to protect information that is critical to the real-time operations of the Bulk Electric System while in transit between applicable Control Centers. The number of plan(s) and their content may depend on a Responsible Entity's management structure and operating conditions. The Responsible Entity may document as many plans as necessary to meet its needs. For instance, a Responsible Entity may choose to document one plan per Control Center or it may choose to document everything in a single plan. A Responsible Entity may choose to document one plan for communications between Control Centers it owns and a separate plan for communications between its Control Centers and the Control Centers of a neighboring Entity. The number and structure of the plans is at the discretion of the Responsible Entity as long as the plan(s) include the required elements described in parts 1.1, 1.2, and 1.3 of Requirement 1.

Identification of Security Protection

Entities have latitude to determine which security protections are used to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring and control data while being transmitted between Control Centers and should identify those protections accordingly.

This security protection could consist of logical protection, physical protection, or some combination of both. To determine security protection, the requirement specifies that it must mitigate the risk of unauthorized disclosure or modification of applicable data.

Identification of Demarcation Point(s)

A Responsible Entity should consider its environment to determine an effective solution when identifying the demarcation points where security protections are applied. One approach to identifying a demarcation point is to place the demarcation point within the Control Center so the confidentiality and integrity of the data is protected throughout the transmission. The Responsible Entity can choose either a physical or logical demarcation point. Demarcation points identified by the Responsible Entity do not add additional assets to the scope of the CIP Reliability Standards. The demarcation point identification ensures that each Responsible Entity identifies clear demarcation of where the protection is applied to the in-scope data. Demarcation points may vary based on many factors such as impact levels of the Control Center, different technologies, or infrastructures.

Identification of Roles and Responsibilities when the Control Centers are Owned or Operated by Different Responsible Entities

The Technical Rationale and Justification for CIP-012-1 identifies key considerations in the Control Center Ownership section when communicating between Control Centers with different owners or operators. Most if not all of the many relationships between Responsible Entities are unique. Consequently, there is no single way to identify roles and responsibilities for applying security protection to the transmission of Real-time Assessment and Real-time monitoring and control data between Control Centers. Responsible Entities may consider identifying the roles and responsibilities for the following situations: (1) configuration of security protocols, (2) responding to communication failures, and (3) responding to Cyber Security Incidents.

General Considerations for R2

Given the format of the requirements, the majority of the documentation is required under R1 while R2 requires the implementation of the plan developed for R1. Compliance with R2 is established by implementing the protection identified in a Responsible Entity's R1 plan. The sections below outline examples of evidence that may be provided in order to demonstrate the implementation of Entity Alpha's CIP-012-1 R1 plan.

Identification of Security Protection

Implementation of the security protection can be demonstrated in many ways. If physical protection is used, a Responsible Entity may demonstrate implementation through a floor plan which identifies the physical security measures in place protecting the communication link. If logical protection is used, a Responsible Entity may demonstrate implementation through an export of the device configuration which applies the security protection. Alternatively, a Responsible Entity may demonstrate implementation through monitoring of the security control such as a report generated from an automated tool that monitors the encryption service used to protect a communications link.

Identification of Demarcation Point(s)

Identification of demarcation point(s) could be demonstrated with a diagram (physical or logical) or a list. This diagram or list could be included within the plan developed for R1. A label could also be used to identify a device as a demarcation point.

Identification of Roles and Responsibilities when the Control Centers are Owned or Operated by Different Responsible Entities

Implementation of roles and responsibilities could also be demonstrated in many ways. Some examples include a joint procedure, a memorandum of understanding or meeting minutes between the two parties where roles and responsibilities are discussed.

Reference Models

For this Implementation Guidance, the SDT considers a basic reference model of Primary and Backup Control Centers (Entity Alpha) to illustrate concepts necessary to demonstrate compliance. These Control Centers communicate to each other and to a neighboring entity's Control Center (Entity Beta) in configurations outlined by the diagrams in this section. The SDT recognizes that the reference models do not contain many of the complexities of a real Control Center. For this Implementation Guidance, the registration or functions performed in the reference model Control Center are also not considered. A high level block diagram of the basic reference model is shown below in Figure 1. This Implementation Guidance is developed from the perspective of Entity Alpha.

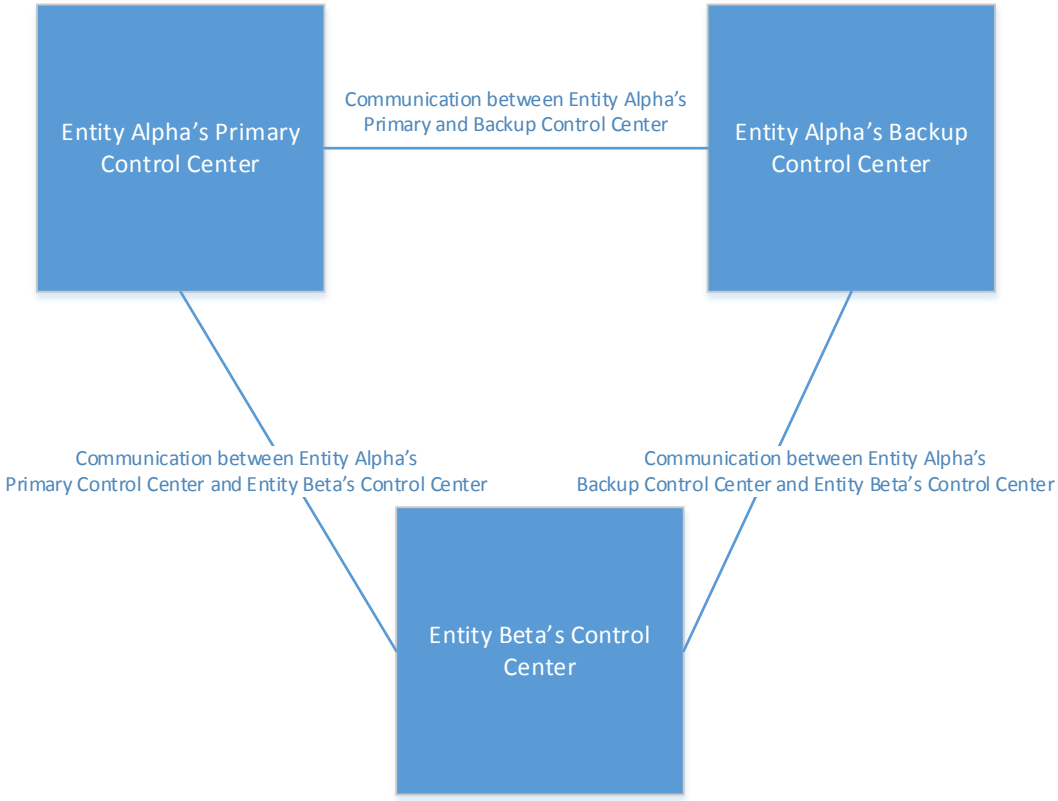


Figure 1: High Level Block Diagram of Reference Model Control Centers

Reference Model Discussion for Requirement R1

Requirement R1 requires the development of a documented plan. To comply with requirement R1, one approach to a plan is to first determine which communications require protection pursuant to CIP-012-1. There are multiple ways to identify an entity's scope in R1. For example, Entity Alpha in the reference model may first identify the Control Centers with which it communicates. Entity Alpha would determine that there are three: Entity Alpha's Primary Control Center, Entity Alpha's Backup Control Center, and Entity Beta's Control Center. Entity Alpha does not need to consider whether Entity Beta further shares its data with another Entity. That is the responsibility of Entity Beta and is outside of Entity Alpha's purview. Additionally, Entity Alpha does not need to consider any communications to other non-Control Center facilities such as generating plants or substations. These communications are out of scope for CIP-012-1.

Now that Entity Alpha has identified the Control Centers with which it communicates, Entity Alpha identifies either: (1) the Real-time Assessment and Real-time monitoring and control data; or (2) communication links which are used to transmit Real-time Assessment and Real-time monitoring and control data between Control Centers. In either case, Entity Alpha may find it useful to refer to the data specification for Real-time

Assessment and Real-time monitoring data identified in TOP-003-3 and IRO-010-2. For this reference model scenario, identifying the communication links used to transmit Real-time Assessment and Real-time monitoring and control data may be the most straightforward approach. Through an evaluation of communication links between Control Centers and an evaluation of how it transmits and receives Real-time Assessment and Real-time monitoring and control data, Entity Alpha determined that it communicates applicable data between its primary and backup Control Centers across a single communication link. Entity Alpha also determined that it communicates applicable data to and from Entity Beta's Control Center across one of two links that originate from either Entity Alpha's primary or backup Control Center using the Inter-Control Center Communications Protocol (ICCP).

With an identified scope of communications links, Entity Alpha now considers the three required elements of its required communications between Control Centers for its plan.

Identification of Security Protection

- Entity Alpha must ensure that protection is applied at the CIP-012-1 demarcation point. The protection must also meet the security objective of mitigating the risk of unauthorized disclosure or modification of applicable data while in transit between Control Centers for the entire distance between CIP-012-1 demarcation points. In a simple case where the demarcation point is sufficiently close to the Control Center, such as within the Physical Security Perimeter of the Control Center, Entity Alpha may use a single security protection method to meet the security objective. For this case, shown in Figure 2, Entity Alpha documents in its plan that it uses a Virtual Private Network (VPN) connection across a private leased communication circuit for each of its three in-scope communication links. To meet the security objective, Entity Alpha further states that its VPN uses Internet Protocol security (IPsec) with AES-128 encryption.
- For more complex scenarios, Entity Alpha may need to use a combination of security controls. For instance, in Figure 3, Entity Alpha uses a combination of physical security controls (physical access control) and logical security controls (encrypted communications consistent with the first scenario above) to meet the security objective.
- The complexity increases when Entity Alpha and Entity Beta exchange data through a 3rd party, such as in Figure 4. In this scenario, Entity Alpha again uses a combination of logical controls. First, encrypted communications are used between the CIP-012-1 demarcation point at Entity Alpha and extended to the 3rd party WAN router. Then, a number of security controls may be leveraged such as network segmentation and system access control to protect the data as it transits the 3rd party network. Finally, encrypted communications is used again to protect the data as it transits between the 3rd party network and the CIP-012-1 demarcation point at Entity Beta.
- While these scenarios are all specific to communication links, it is possible that Entity Alpha and Entity Beta achieve the security objective by applying protection to the data rather than the communication links. In this scenario, the application enabling the data exchange between Control Centers may be capable of applying security controls directly to the data. These security controls mitigate the risk of unauthorized disclosure or modification of applicable data rather than relying on lower level network services to provide this security. For instance, Entity Alpha and Entity Beta may apply security protection at the application layer by using Secure ICCP to exchange applicable data. According to a report released by Sandia National Labs[2], Secure ICCP provides "data integrity indirectly by providing a cryptographic checksum…Secure ICCP provides data confidentiality by encrypting ICCP data exchanges." Methods other than Secure ICCP could also be used to apply security protection to the data at the application layer.
- It is theoretically possible that Entity Alpha and Entity Beta could exchange Real-time Assessment data between Control Centers by email. In that scenario, one approach may be for Entity Alpha to email the

[2] https://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/19-Secure_ICCP_Integration.pdf

applicable data to Entity Beta's Control Center in a protected container such as an encrypted zip file. Entity Alpha and Entity Beta can then exchange the password to that encrypted container through another method, such as by phone. While the notional example of protecting data exchanged by email is a useful illustration of how to achieve the security objective of CIP-012-1, it is extremely unlikely to be used in practice. The characteristics of email communication are inconsistent with the requirements of Real-time data exchange.

Identification of Demarcation Point(s)

- Figure 2 shows the identification of CIP-012-1 demarcation points for the Entity Alpha reference model. Entity Alpha has identified its demarcation point at each of its Control Centers to be the external Ethernet interface on the WAN router where the security protection is applied. It has also coordinated with Entity Beta to identify a similar demarcation point at Entity Beta's Control Center.
- In some cases, it may be helpful to identify both the CIP-012-1 demarcation points and the telecommunications carrier (telco) demarcation point. Figure 3 provides such an example where the telco demarcation point may not be within the Control Center. In this scenario, Entity Alpha identifies the CIP-012-1 demarcation point to be a point on the communications path adjacent to the outside interface on the ESP firewall. Entity Alpha has also identified the telco demarcation point at a point in the telecommunications cabling connecting to Entity Alpha's WAN router, perhaps at a punch down block for example. In Figure 3, the telco demarcation point is inside the same room as the WAN router. The telco demarcation points are referenced in the drawing for clarity, but are not part of the plan.
- Figure 4 shows the identification of possible CIP-012-1 demarcation points and telco demarcation points when Entity Alpha and Entity Beta transmit the applicable data through a third party.
- The data-centric scenario described above is less intuitive for identifying demarcation points. If security protection is applied at the application layer (such as Secure ICCP), Entity Alpha could reasonably identify the application or service applying the security (such as the Secure ICCP service) as the demarcation point.

Identification of Roles and Responsibilities when the Control Centers are Owned or Operated by Different Responsible Entities

Entity Alpha and Entity Beta may determine they each are responsible for one end of the VPN configuration on their respective WAN routers. Entity Alpha and Entity Beta have agreed to a 30 character pre-shared key for IPSec authentication and have exchanged contact information for their Network Operations Centers to enable a coordinated response to any communication failures. They have also exchanged contact information for their Security Operations Centers to enable a coordinated response to any suspected Cyber Security Incidents.

Rather than use a pre-shared key, Entity Alpha and Entity Beta may decide to use digital certificates for the IPSec authentication using a trusted certificate authority. In that scenario, Entity Alpha and Entity Beta would agree on who is the party responsible for managing the certificate authority.

When using a third party as shown in Figure 4, Entity Alpha and Entity Beta will need to define who is responsible for each part of the connection between them. Each entity may determine they are responsible for only the connection from their CIP-012-1 demarcation point to the telco demarcation point at the 3rd party. The 3rd party may take responsibility for protecting the data transiting its network.

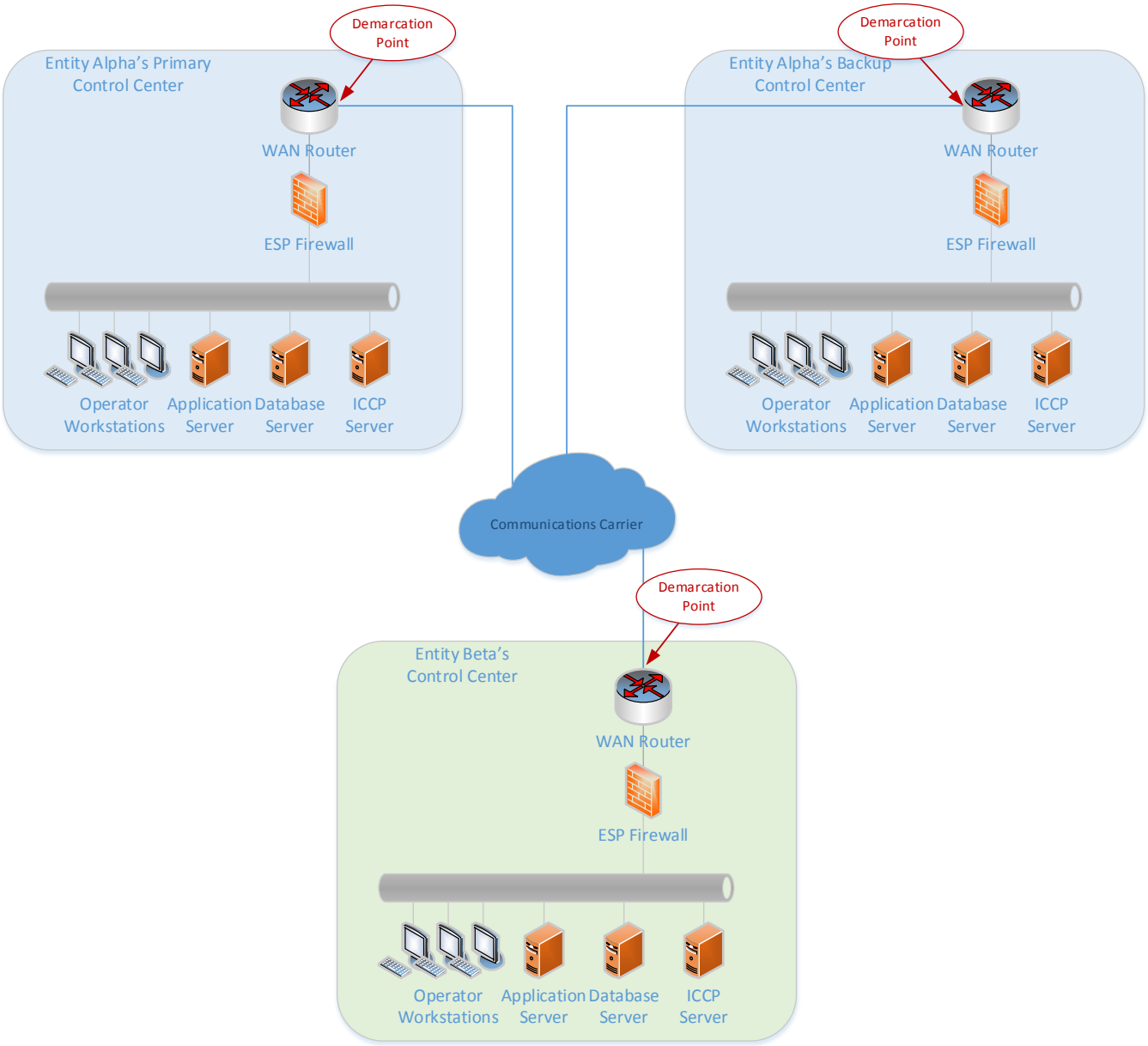


Figure 2: Network diagram and identification of demarcation points

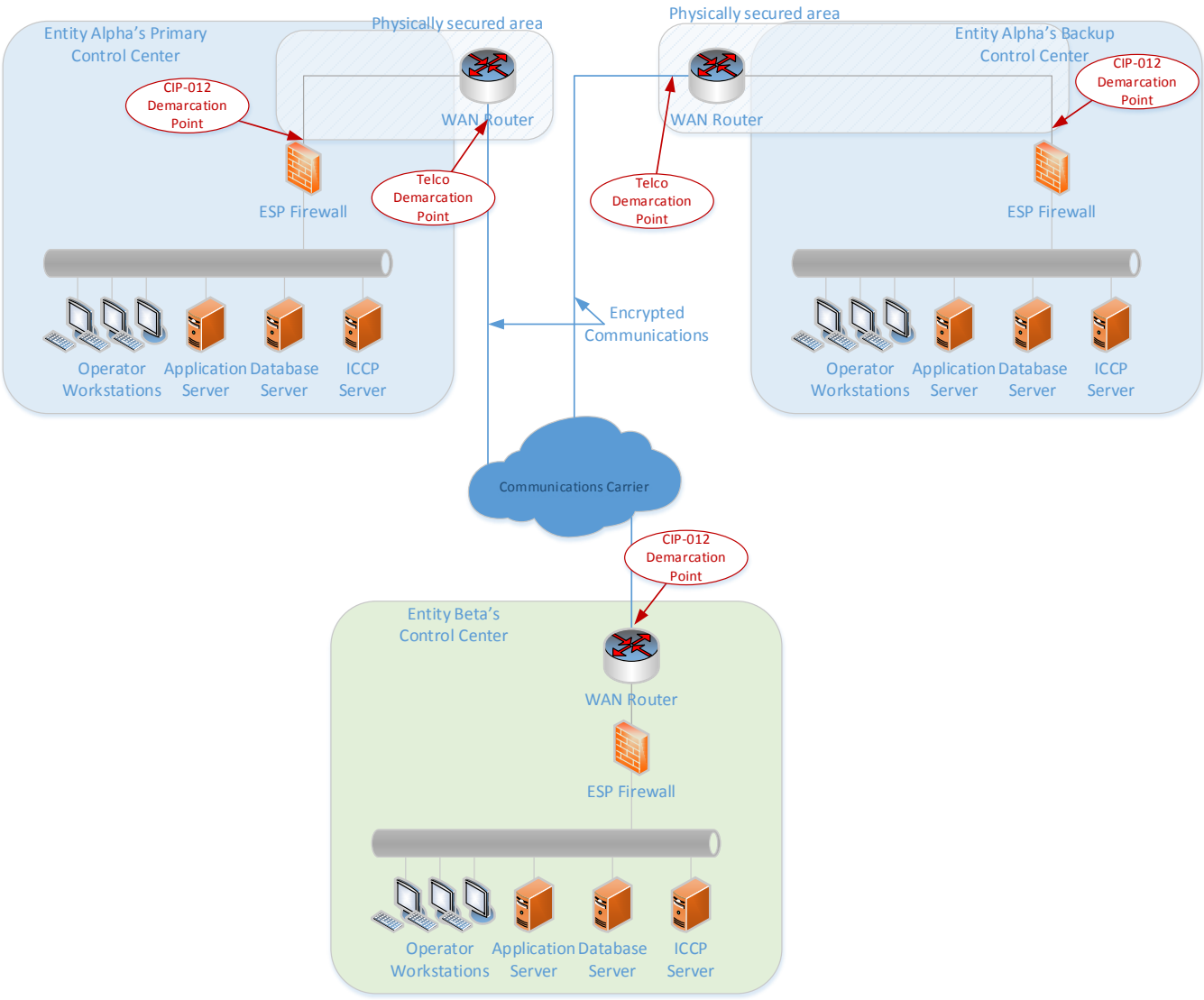


Figure 3: Network diagram using a combination of controls for CIP-012-1

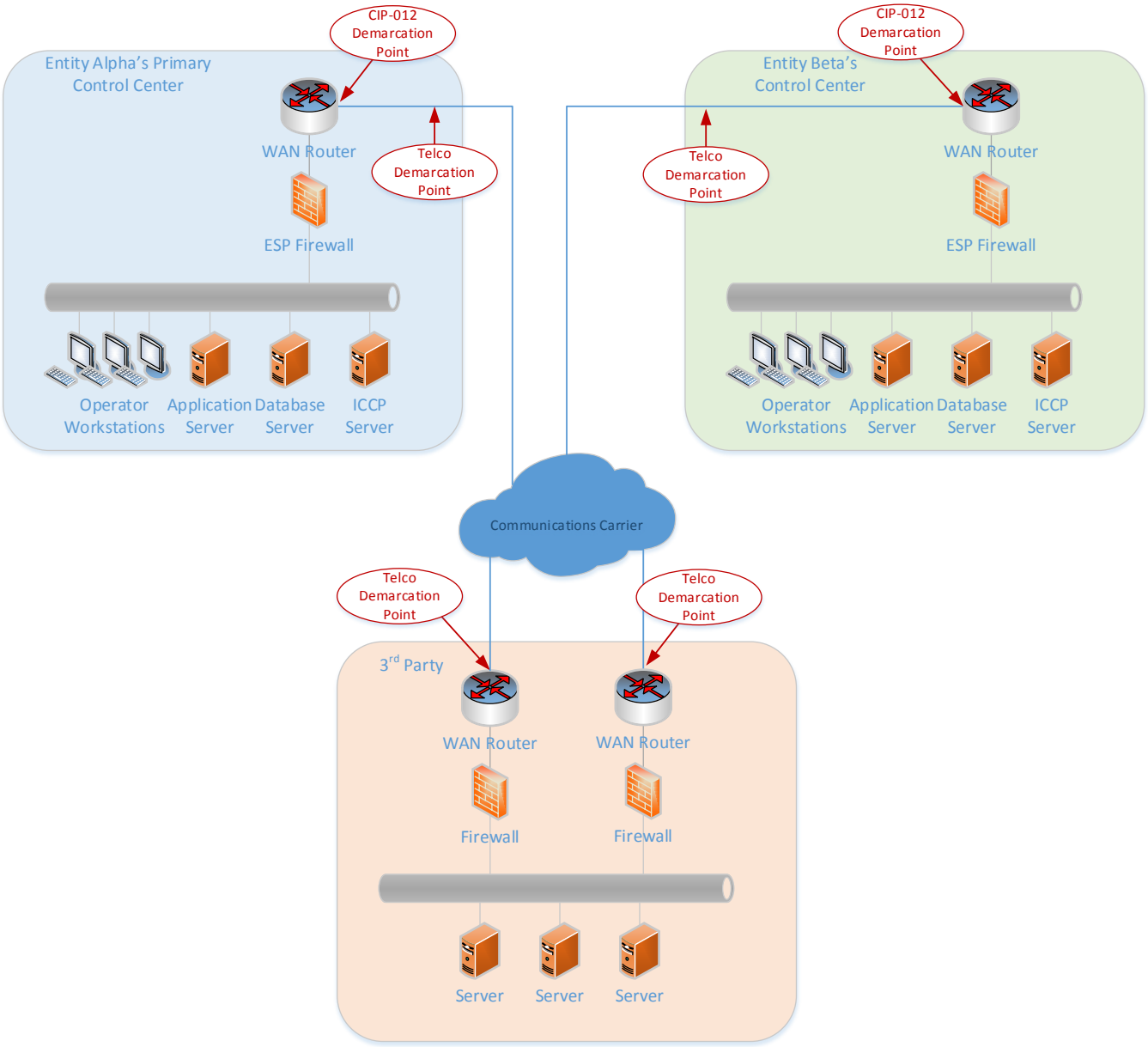


Figure 4: Network Diagram depicting communications through a 3rd party

Reference Model Discussion for Requirement R2

Entities must demonstrate implementation of their R1 plan. The sections below outline examples of evidence that may be provided to demonstrate the implementation of Entity Alpha's CIP-012-1 R1 plan.

Identification of Security Protection

Entity Alpha may demonstrate security protection implementation through the WAN router configuration which shows that a site-to-site IPSec VPN with AES-128 encryption is in place.

When physical security controls are used, Entity Alpha may demonstrate the implementation of physical protection using a floorplan diagram showing the physical access controls in place.

Identification of Demarcation Point(s)

Entity Alpha may demonstrate the identification of demarcation points through a network diagram very similar to that shown in Figure 2.

Identification of Roles and Responsibilities when the Control Centers are Owned or Operated by Different Responsible Entities

Entity Alpha may demonstrate the implementation of roles and responsibilities with Entity Beta through a memorandum of understanding (MOU) signed by both parties.

References

Mitre Common Weakness Enumeration (CWE™) list of software weakness types
https://cwe.mitre.org/data/definitions/327.html

Cryptographic Standards and Guidelines
https://csrc.nist.gov/Projects/Cryptographic-Standards-and-Guidelines

NIST Special Publication 800-175B
Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-175B.pdf

Guide to Cryptography
https://www.owasp.org/index.php/Guide_to_Cryptography#Symmetric_Cryptography

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Comment Form

Project 2016-02 Modifications to CIP Standards
CIP-012-1

Do not use this form for submitting comments. Use the Standards Balloting and Commenting System (SBS) to submit comments on the draft **Technical Rationale and Justification** and **Implementation Guidance for CIP-012-1.** Comments must be submitted by **8 p.m. Eastern, Monday, December 11, 2017.**

Additional information is available on the project page. If you have questions, contact Katherine Street at (404) 446-9702 or Mat Bunch at (404) 446-9785.

Background Information

On January 21, 2016, the Commission issued Order No. 822, approving seven CIP Reliability Standards and new or modified definitions, and directing modifications to the CIP Reliability Standards. Among others, the Commission directed NERC to "develop modifications to the CIP Reliability Standards to require responsible entities to implement controls to protect, at a minimum, communication links and sensitive bulk electric system data communicated between bulk electric system Control Centers in a manner that is appropriately tailored to address the risks posed to the bulk electric system by the assets being protected (i.e., high, medium, or low impact)." (Order 822, Paragraph 53)

The Project 2016-02 Standard Drafting Team (SDT) drafted Reliability Standard CIP-012-1 to require Responsible Entities to implement controls to protect sensitive Bulk Electric System (BES) data while being transmitted over communications links between BES Control Centers. Due to the sensitivity of the data being communicated between the Control Centers the standard applies to all impact levels (i.e., high, medium, or low impact).

The SDT drafted Technical Rationale and Justification for Reliability Standard CIP-012-1 to explain the technical rationale for the proposed Reliability Standard. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. It also contains information on the SDT's intent in drafting the requirements.

The SDT also drafted Implementation Guidance to provide examples of approaches to comply with CIP-012-1. Implementation Guidance does not prescribe the only approach, but is intended to highlight one or more approaches that would be effective ways to be compliant with the standard. As Implementation Guidance is only meant to provide examples, entities may choose alternative approaches that better fit their situation.

Questions

1. The SDT developed draft Technical Rationale and Justification for CIP-012 to assist in understanding the technology and technical requirements in the Reliability Standard. It also contains information on the SDT's intent in drafting the requirements. Do you agree with the technology and technical requirements in the draft Technical Rationale and Justification? If you do not agree, or if you agree but have comments or suggestions for the draft Technical Rationale and Justification, please provide your recommendation and explanation.

   ☐ Yes
   ☐ No

   Comments:

2. The SDT developed draft Implementation Guidance for CIP-012 to provide examples of how a Responsible Entity could comply with the requirements. The draft Implementation Guidance does not prescribe the only approach to compliance. Rather, it describes some approaches the SDT believes would be effective ways to comply with the standard. See NERC's Compliance Guidance policy for information on Implementation Guidance. Do you agree with the example approaches in the draft Implementation Guidance? If you do not agree, or if you agree but have comments or suggestions for the draft Implementation Guidance, please provide your recommendation and explanation.

   ☐ Yes
   ☐ No

   Comments:

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

2016-02 Modifications to CIP Standards

Informal Comment Period Open through December 11, 2017

Now Available

An informal comment period is open through **8 p.m. Eastern, Monday, December 11, 2017**, for stakeholders to provide feedback on the draft **Technical Rationale and Justification** and **Implementation Guidance for CIP-012-1**.

Commenting

Use the Standards Balloting and Commenting System (SBS) to submit comments. If you experience difficulty navigating the SBS, contact Wendy Muller. An unofficial Word versions of the comment form is posted on the project page.

If you are having difficulty accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out, contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern).

- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*
- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Next Steps

The drafting team will review all responses received and determine the next steps of the project.

For more information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact Katherine Street at (404) 446-9702 or Mat Bunch at (404) 446-9785.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Comment Report

Project Name:	2016-02 Modifications to CIP Standards | Technical Rationale and Justification and Implementation Guidance for CIP-012-1
Comment Period Start Date:	11/20/2017
Comment Period End Date:	12/11/2017
Associated Ballots:	

There were 30 sets of responses, including comments from approximately 84 different people from approximately 59 companies representing 10 of the Industry Segments as shown in the table on the following pages.

Questions

1. The SDT developed draft Technical Rationale and Justification for CIP-012 to assist in understanding the technology and technical requirements in the Reliability Standard. It also contains information on the SDT's intent in drafting the requirements. Do you agree with the technology and technical requirements in the draft Technical Rationale and Justification? If you do not agree, or if you agree but have comments or suggestions for the draft Technical Rationale and Justification, please provide your recommendation and explanation.

2. The SDT developed draft Implementation Guidance for CIP-012 to provide examples of how a Responsible Entity could comply with the requirements. The draft Implementation Guidance does not prescribe the only approach to compliance. Rather, it describes some approaches the SDT believes would be effective ways to comply with the standard. See NERC's Compliance Guidance policy for information on Implementation Guidance. Do you agree with the example approaches in the draft Implementation Guidance? If you do not agree, or if you agree but have comments or suggestions for the draft Implementation Guidance, please provide your recommendation and explanation.

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
SRC & SWG	David Francis	2	FRCC,MRO,NPCC,RF,SERC,SPP RE,Texas RE,WECC	SRC + SWG	Gregory Campoli	New York Independent System Operator	2	NPCC
					Mark Holman	PJM Interconnection, L.L.C.	2	RF
					Charles Yeung	Southwest Power Pool, Inc. (RTO)	2	SPP RE
					Terry BIlke	Midcontinent ISO, Inc.	2	RF
					Elizabeth Axson	Electric Reliability Council of Texas, Inc.	2,3	Texas RE
					Ben Li	IESO	1	MRO
					Drew Bonser	SWG	NA - Not Applicable	NA - Not Applicable
					Darrem Lamb	CAISO	2	WECC
					Matt Goldberg	ISONE	2	NPCC
Seattle City Light	Ginette Lacasse	1,3,4,5,6	WECC	Seattle City Light Ballot Body	Pawel Krupa	Seattle City Light	1	WECC
					Hao Li	Seattle City Light	4	WECC
					Bud (Charles) Freeman	Seattle City Light	6	WECC
					Mike Haynes	Seattle City Light	5	WECC
					Michael Watkins	Seattle City Light	1,4	WECC
					Faz Kasraie	Seattle City Light	5	WECC
					John Clark	Seattle City Light	6	WECC
					Tuan Tran	Seattle City Light	3	WECC
					Laurrie Hammack	Seattle City Light	3	WECC

Public Utility District No. 1 of Chelan County	Janis Weddle	1,3,5,6		Chelan PUD	Haley Sousa	Public Utility District No. 1 of Chelan County	5	WECC
					Joyce Gundry	Public Utility District No. 1 of Chelan County	3	WECC
					Jeff Kimbell	Public Utility District No. 1 of Chelan County	1	WECC
					Janis Weddle	Public Utility District No. 1 of Chelan County	6	WECC
DTE Energy - Detroit Edison Company	Karie Barczak	3,4,5		DTE Energy - DTE Electric	Jeffrey Depriest	DTE Energy - DTE Electric	5	RF
					Daniel Herring	DTE Energy - DTE Electric	4	RF
					Karie Barczak	DTE Energy - DTE Electric	3	RF
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,8,9,10	NPCC	RSC no Dominion and ISO-NE	Guy V. Zito	Northeast Power Coordinating Council	10	NPCC
					Randy MacDonald	New Brunswick Power	2	NPCC
					Wayne Sipperly	New York Power Authority	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	Orange & Rockland Utilities	3	NPCC
					Michele Tondalo	UI	1	NPCC
					Laura Mcleod	NB Power	1	NPCC

					David Ramkalawan	Ontario Power Generation Inc.	5	NPCC
					Quintin Lee	Eversource Energy	1	NPCC
					Paul Malozewski	Hydro One Networks, Inc.	3	NPCC
					Helen Lainis	IESO	2	NPCC
					Michael Schiavone	National Grid	1	NPCC
					Michael Jones	National Grid	3	NPCC
					Greg Campoli	NYISO	2	NPCC
					Sylvain Clermont	Hydro Quebec	1	NPCC
					Chantal Mazza	Hydro Quebec	2	NPCC
					Silvia Mitchell	NextEra Energy - Florida Power and Light Co.	6	NPCC
					Michael Forte	Con Ed - Consolidated Edison	1	NPCC
					Daniel Grinkevich	Con Ed - Consolidated Edison Co. of New York	1	NPCC
					Peter Yost	Con Ed - Consolidated Edison Co. of New York	3	NPCC
					Brian O'Boyle	Con Ed - Consolidated Edison	5	NPCC
					Sean Cavote	PSEG	4	NPCC
Southwest Power Pool, Inc. (RTO)	Shannon Mickens	2	SPP RE	SPP Standards Review Group	Shannon Mickens	Southwest Power Pool Inc.	2	SPP RE
					Megan Wagner	Westar Energy	6	SPP RE
					Louis Guidry	Cleco Corporation	1,3,5,6	SPP RE
					Robert Gray	Board of Public Utilities (BPU), Kansas City, KS	NA - Not Applicable	NA - Not Applicable

					Ron Spicer	EDF Renewables	5	SPP RE

1. The SDT developed draft Technical Rationale and Justification for CIP-012 to assist in understanding the technology and technical requirements in the Reliability Standard. It also contains information on the SDT's intent in drafting the requirements. Do you agree with the technology and technical requirements in the draft Technical Rationale and Justification? If you do not agree, or if you agree but have comments or suggestions for the draft Technical Rationale and Justification, please provide your recommendation and explanation.

Janis Weddle - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Chelan PUD

Answer	No
Document Name	

Comment

The technical guidance sections do a suitable job of describing the problem that the SDT is being asked to solve. The rationale for the alignment, however, introduces concern given that the term "Real-time monitoring", while aligned with IRO and TOP terminology, is not itself a NERC-defined term and is also being further modified to create another new "Real-time monitoring and control" undefined term. Given that the term is already being changed, CHPD requests that the STD instead consider creating a new "BES data" (a term used by the SDT in the Draft 2 Unofficial Comment Form) NERC Glossary term to be used to clearly scope the data in question. Here is a potential, admittedly simple, initial definition to consider:

BES Data – Electronic data used by BES Cyber Systems to perform Supervisory Control and Data Acquisition (SCADA).

The intent of the concept of "demarcation points" is well-reasoned and CHPD supports this identification capability. CHPD requests that the Technical Rationale and Justification (TR&J) for this section be more clearly aligned with the Requirement R1.2, which does not currently limit the scope to the Responsible Entity's Control Center. Consider the following revision:

"1.2 Identification of *the Responsible Entity's* demarcation point(s)…"

A change to a demarcation point in one system should not create a paperwork or compliance issue for a neighbor or vice versa. Alternatively, consider defining the term "demarcation point" in the NERC glossary to identify the scope within the definition of the term, rather than in the language of the standard.

Likes 0	
Dislikes 0	

Response

Richard Jackson - U.S. Bureau of Reclamation - 1,5

Answer	No
Document Name	

Comment

Reclamation also recommends the Drafting Team state clearly that examples provided in Technical Rationale and Justification documents are neither mandatory, nor enforceable, nor the only method of achieving compliance.

Likes 0	
Dislikes 0	

Response

Andrew Gallo - Austin Energy - 1,3,4,5,6	
Answer	No
Document Name	
Comment	

Austin Energy (AE) generally agrees with the Draft 2 revision. However, the SDT should define the new terms “monitoring data” and “control data” in the NERC Glossary. Additionally, the concept of “demarcation point(s)” is unclear. The Standard should indicate a Registered Entity should identify the Cyber Asset at which the Entity begins protected data and ceases to protect data. The current wording implies each entity should document its demarcation point and any demarcation point(s) at a neighboring system. A change to a demarcation point for one entity should not create a paperwork or compliance issue for a neighbor. Alternatively, the SDT could define “demarcation point.”

Also, while the Technical Rationale and Justification for CIP-012 addresses R1 (scope, demarcation points, roles and responsibilities), it does not properly address R2. While physical protections may protect confidentiality between Control Centers owned by the same entity, it does not address non-repudiation and, therefore, integrity as defined by NIST 800-53, Revision 4, page B-6. AE asks the SDT to provide additional rationale and justification regarding how the protections are required “…in a manner that reflects the risks posed to bulk electric system reliability,” as stated on page 12 of FERC Order No. 822.

Likes 0	
Dislikes 0	
Response	

Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	
Comment	

N&ST believes the draft Technical Rationale and Justification fails to address the applicability of CIP-012 to the exchange of Real-time Assessment data between a BES Control Center and a third party provider of such data. At the same time, the draft Implementation Guidance document clearly indicates that the SDT believes this scenario would be in scope. If this is in fact true, then both the Technical Rationale and Justification and CIP-012 standard document should include explicit statements to that effect.

Likes 0	
Dislikes 0	
Response	

Don Schmit - Nebraska Public Power District - 1,3,5	
Answer	No
Document Name	

Comment
See comments from the MRO NSRF for the ballot conducted for CIP-012-1 which closed on December 11, 2017.

Likes 0	
Dislikes 0	

Response

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3	
Answer	No
Document Name	

Comment
We do not agree with two separate requirements, one for a plan and one to implement. We recommend following precedent in the other CIP standards, for example, CIP-004-011. The obligation can be accomplished with one requirement, as follows. “The Responsible Entity shall implement one or more documented process(es) to mitigate the risk of the unauthorized disclosure or modification of Real-time Assessments and Real-time monitoring and control data while being transmitted between any Control Centers, except under CIP Exceptional Circumstances. This excludes oral communications. The process(es) shall identify: 1.1 security protection used to mitigate risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring and control data while being transmitted between Control Centers. 1.2 demarcation point(s) where security protection is applied for transmitting Real-time Assessment and Real-time monitoring and control data between Control Centers. Demarcation points identified by the Responsible Entity do not add additional Cyber Assets to the scope of the CIP Reliability Standards; and 1.3 roles and responsibilities of each Responsible Entity for applying security protection to the transmission of Real-time Assessment and Real-time monitoring and control data between Control Centers, when the Control Centers are owned or operated by different Responsible Entities.” This also includes important scoping from the implementation guidance that belongs in the requirement, that demarcation points don’t add additional Cyber Assets to the scope of the CIP standards.

Likes 0	
Dislikes 0	

Response

Lona Calderon - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	

Comment
While the Technical Rationale and Justification for CIP-012 goes into great detail for R1 to give an understanding and overview of the rationale behind the scope, demarcation points, and the need for roles and responsibilities, SRP asserts it did not properly address Requirement 2. While physical protections may satisfy the objective of protecting confidentiality between Control Centers owned by the same Registered Entity, it does not address non-repudiation in any situation, and therefore integrity as it was defined by NIST 800-53, Revision 4, page B-6. SRP requests the SDT

provide more rationale and justification as to how these protections are being required "…in a manner that reflects the risks posed to bulk electric system reliability," as stated on page 12 of FERC Order No. 822.

Likes 0	
Dislikes 0	

Response

Annette Johnston - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3

Answer	No
Document Name	

Comment

Support Terry Harbour comments (Berhshire Hathaway Company - MidAmerican Energy Company)

Likes 0	
Dislikes 0	

Response

Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	No
Document Name	

Comment

CenterPoint Energy Houston Electric, LLC ("CenterPoint Energy") does not agree with certain comments in the draft Technical Rationale and Justification. As detailed in its Comment Form for proposed CIP-012-1, CenterPoint Energy recommends that the phrase "and control" be removed from proposed Requirement R1 on page 4 of the draft Technical Rationale and Justification. Inclusion of this phrase may create confusion and does not align with TOP-003 and IRO-010 data specification Requirements. Additionally, the phrase was not mentioned in FERC Order 822. Thus, CenterPoint Energy recommends corresponding revisions to the Technical Rational and Justification.

The SDT's justification on page 5 of the draft Technical Rationale and Justification for adding "and control" to "Real-time monitoring and control data" is unclear and confusing. The SDT recognizes that "in practice Real-time control data is not transmitted separately from Real-time monitoring data." Given this practice, the introduction of the concept of separately transmitted "Real-time control data" may create confusion on whether there are additional data specification responsibilities besides those detailed in TOP-003 and IRO-010.

To align with the revisions recommended above and in its Comment Form for proposed CIP-012-1, CenterPoint Energy also recommends that the following sentences be removed from the first paragraph of page 5 of the draft Technical Rationale and Justification:

"The SDT notes that it expanded the phrase 'Real-time monitoring' from TOP-003 and IRO-010 to 'Real-time monitoring and control' data."

"However, the SDT wanted to ensure that Real-time control data was included regardless of whether or not it is transmitted along with Real-time monitoring data."

CenterPoint Energy believes the rest of the first paragraph on page 5 is appropriate to be included because it states the SDT's thought process and concern.	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE	
Answer	No
Document Name	
Comment	
Under the General Considerations section of the Technical Rationale, Xcel Energy has concerns with implementation of this Standard as related to the term and definition of Control Center. Specifically, we are concerned with the definition of an "associated data center" as part of the Control Center. The Standard does not appear to apply to communication between the control center and a field device (per reference model on page 5 of Technical Rationale). However, if we have a Control Center communicating with a device that aggregates multiple field devices, is that aggregating device location considered an associated data center? Under the Alignment with IRO and TOP Standards, we believe that the types of data to be within scope, as identified by data specification lists originating from TOP-003 and IRO-010 are not specific enough to determine or limit the types of data or communication methods that would need to be protected as Real Time Assessments, Real Time Monitoring, or Control Data. These lists contain data and methods of communicating data that Xcel Energy would not classify as Real Time Assessment, Real Time Monitoring, or Control Data. Xcel Energy's concern is that NERC and Regional Entities may. The inclusion of all data types and methods on these lists could bring systems like corporate email into scope, which we would adamantly oppose. We suggest adding further clarification as to what types of data are included as Real Time Assessment, Real Time Monitoring, and Control Data.	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	No
Document Name	
Comment	
We support SRP and Chelan PUD comments.	
Likes 0	
Dislikes 0	
Response	

Rick Applegate - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6	
Answer	No
Document Name	
Comment	

Tacoma Power endorses the draft comments shared with it by Salt River Project (SRP), which follow:

While the Technical Rationale and Justification for CIP-012 goes into great detail for R1 to give an understanding and overview of the rationale behind the scope, demarcation points, and the need for roles and responsibilities, SRP asserts it did not properly address Requirement 2.

While physical protections may satisfy the objective of protecting confidentiality between Control Centers owned by the same Registered Entity, it does not address non-repudiation in any situation, and therefore integrity as it was defined by NIST 800-53, Revision 4, page B-6. SRP requests the SDT provide more rationale and justification as to how these protections are being required "…in a manner that reflects the risks posed to bulk electric system reliability," as stated on page 12 of FERC Order No. 822.

Likes 0	
Dislikes 0	
Response	

John Tolo - Unisource - Tucson Electric Power Co. - 1	
Answer	Yes
Document Name	
Comment	

This is reasonable given that some of the communications may flow on third-party networks. That said, there seems to be no discussion of protecting the communications devices themselves. Recommend taking a "high watermark" approach to categorizing the importance and risk of communication systems. Many utilities use internal communications between their PCC and BCC. If those links are not trusted and require the protections of CIP-012, why trust the substation SCADA links feeding data to the control centers? Being more prescriptive would be helpful. Is the SDT mandating encryption? What physical protections would be sufficient? Is OPGW fiber "protected" or just "difficult?"

Likes 0	
Dislikes 0	
Response	

Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	

Page 5 (Control Center Ownership) - Recommend changing ‘ensure adequate protection is applied’ to ‘ensure the security objective is met’ in the sentence, *‘It is strongly recommended, however, that these partnering entities develop agreements, or use existing ones, to define responsibilities to ensure adequate protection is applied.’*

Likes 0	
Dislikes 0	

Response

Richard Vine - California ISO - 2

Answer	Yes
Document Name	

Comment

The California ISO supports the comments of the IRC Security Working Group (SWG)

Likes 0	
Dislikes 0	

Response

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group

Answer	Yes
Document Name	

Comment

The SPP Standards Review Group proposes to include the defined terms “Confidentiality” and “Integrity” in the NERC Glossary of Terms or, at a minimum, define the terms in the body of the standard. The current definitions are stated in the National Institute of Standards and Technology’s (NIST) Special Publication 800-53A, Revision 4 (as footnoted in the Technical Rationale Documentation); however, the NIST document is non-governing and could be revised outside the purview of NERC, which could have a negative impact on an entity’s compliance with standards such as CIP-012. The SPP Standards Review Group would recommend utilizing the definitions for “Confidentiality” and “Integrity” as stated in the current Technical Rational and Justification for CIP-012.

Additionally, the SPP Standards Review Group would recommend the same course of action be applicable to the term “Demarcation Point.”

Likes 0	
Dislikes 0	

Response

Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2

Answer	Yes
Document Name	
Comment	
ERCOT signs onto the comments of the SRC/ITC/SWG of the IRC, pasted below. The SRC & ITC SWG offers the following comments and recommendations. To solidify the intent of the SDT, as noted in the response to comments, the SRC & ITC SWG recommend that it be clarified in the Technical Rationale and Justification that CIP-012-1 is a standalone Standard similar to CIP-014 and is not intended to increase the scope of applicable systems to be protected under CIP-003 thru CIP-011.	
Likes 0	
Dislikes 0	
Response	
David Francis - SRC & SWG - 2 - MRO,NPCC,SERC,RF, Group Name SRC + SWG	
Answer	Yes
Document Name	
Comment	
Comments: The SRC & ITC SWG offers the following comments and recommendations. To solidify the intent of the SDT, as noted in the response to comments, the SRC & ITC SWG recommend that it be clarified in the Technical Rationale and Justification that CIP-012-1 is a standalone Standard similar to CIP-014 and is not intended to increase the scope of applicable systems to be protected under CIP-003 thru CIP-011.	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Glen Farmer - Avista - Avista Corporation - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eleanor Ewry - Puget Sound Energy, Inc. - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1,3,5,6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Laurie Williams - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	Yes
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	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Ramkalawan - Ontario Power Generation Inc. - 5	
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	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion and ISO-NE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brandon Cain - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - FRCC,MRO,WECC,Texas RE,SERC,SPP RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	

Texas RE is concerned about the use of the term “or” as used in Requirement R1. Please see Texas RE's comments for Question #1 on the unofficial comment form for the comment period ending on December 11, 2017.

Texas RE also has a concern about the difference between monitoring and control data. On page 5 of the Technical Rationale, the SDT notes that it expanded the phrase “Real-time monitoring” data from TOP-003 and IRO-010 to “Real-time monitoring and control” data. The SDT was concerned that data transmitted between Control Centers that results in the physical operation of BES Elements was not explicitly included in Real-time monitoring data. The SDT understands that in practice Real-time control data is not transmitted separately from Real-time monitoring data. However, the SDT wanted to ensure that Real-time control data was included regardless of whether or not it is transmitted along with Real-time monitoring data. If entities only transmit Real-time control data along with Real-time monitoring data, then the SDT does not intend for such entities to identify additional data beyond that Real-time monitoring data already included in the data specifications for TOP-003 and IRO-010. Texas RE is concerned that if there is a need to expand the phrase to include control data in CIP-012-1, there might also be a need in IRO-010 and TOP-003.

Likes 0	
Dislikes 0	

Response

2. The SDT developed draft Implementation Guidance for CIP-012 to provide examples of how a Responsible Entity could comply with the requirements. The draft Implementation Guidance does not prescribe the only approach to compliance. Rather, it describes some approaches the SDT believes would be effective ways to comply with the standard. See NERC's Compliance Guidance policy for information on Implementation Guidance. Do you agree with the example approaches in the draft Implementation Guidance? If you do not agree, or if you agree but have comments or suggestions for the draft Implementation Guidance, please provide your recommendation and explanation.

Rick Applegate - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6	
Answer	No
Document Name	

Comment

Tacoma Power endorses the draft comments shared with it by Salt River Project (SRP), which follow:

The Implementation Guidance states "The protection must also meet the security objective of mitigating the risk of unauthorized disclosure or modification of applicable data while in transit between Control Centers for the entire distance between CIP-012-1 demarcation points." The document also describes a situation where Entity Alpha exchanges data with Entity Beta through a "3rd party network." The guidance asserts "a number of security controls may be leveraged such as network segmentation and system access control to protect the data as it transits the 3rd party network." However, the document does not describe the implications if the third part circumvents these controls. Additionally, these controls within the 3rd party network do not address non-repudiation, and therefore integrity as it was defined by NIST 800-53, Revision 4, page B-6. SRP asserts more explanation is required within the Implementation Guidance to explain how the example approaches satisfy the security objective. If the approaches indeed satisfy the security objective, then the requirement must be updated to fit the scenario.

Although the SDT states it does not specify controls, the only examples provided in the implementation guidance includes encryption. If there are other methods available other than encryption to achieve the security objective, please provide them.

Likes 0	
Dislikes 0	

Response

Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	No
Document Name	

Comment

We support SRP and Chelan PUD comments.

Likes 0	
Dislikes 0	

Response

Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	No
Document Name	
Comment	

For the same reasons discussed in its Response to Question No. 1 and in its Comment Form for proposed CIP-012-1, CenterPoint Energy recommends that the phrase “and control” be removed from Requirement R1on page 4 of the draft Implementation Guidance..

In accordance with Requirement R1.3, Responsible Entities are required to identify roles and responsibilities for applying security protections. However, on page 5 of the Implementation Guidance, consideration of the following situations was listed: (1) configuration of security protocols, (2) responding to communication failures, and (3) responding to Cyber Security Incidents. Items (2) and (3) go beyond the scope of Requirement R1.3 and, therefore, should be removed from the Implementation Guidance.

Similarly, on page 9, the following example goes beyond the scope of Requirement 1.3 and should be removed from the Implementation Guidance:

“Entity Alpha and Entity Beta have agreed to a 30 character pre-shared key for coordinated response to any communication failures. They have also exchanged contact information for their Security Operations Centers to enable a coordinated response to any suspected Cyber Security Incidents.”

Page 8 and page 13 lists “AES-128 encryption” as an example of protection; however, 128 bit encryption is the lowest key length. CenterPoint Energy recommends removing “AES-128” and only stating the word “encryption.”

In the last paragraph of page 9, regarding communications through a third party, the Implementation Guidance should recommend stronger controls around protecting the data being transmitted through a third party communication link. For example, Entity Alpha and Entity Beta should establish agreements with the 3rd party responsible for the communication to protect the data transiting its network. The last sentence, “The 3rd party may take responsibility for protecting the data transiting its network” does not allow for adequate protection of the data.

Likes 0	
Dislikes 0	
Response	

Annette Johnston - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3

Answer	No
Document Name	
Comment	

Support Terry Harbour comments (Berhshire Hathaway Company - MidAmerican Energy Company)

Likes 0	
Dislikes 0	
Response	

Lona Calderon - Salt River Project - 1,3,5,6 - WECC

Answer	No

Document Name	

Comment

The Implementation Guidance states “The protection must also meet the security objective of mitigating the risk of unauthorized disclosure or modification of applicable data while in transit between Control Centers for the entire distance between CIP-012-1 demarcation points.” The document also describes a situation where Entity Alpha exchanges data with Entity Beta through a “3rd party network.” The guidance asserts “a number of security controls may be leveraged such as network segmentation and system access control to protect the data as it transits the 3rd party network.” However, the document does not describe the implications if the third part circumvents these controls. Additionally, these controls within the 3rd party network do not address non-repudiation, and therefore integrity as it was defined by NIST 800-53, Revision 4, page B-6. SRP asserts more explanation is required within the Implementation Guidance to explain how the example approaches satisfy the security objective. If the approaches indeed satisfy the security objective, then the requirement must be updated to fit the scenario.

Although the SDT states it does not specify controls, the only examples provided in the implementation guidance includes encryption. If there are other methods available other than encryption to achieve the security objective, please provide them.

Likes 0	
Dislikes 0	

Response

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3

Answer	No
Document Name	

Comment

We do not agree with two separate requirements, one for a plan and one to implement. We recommend following precedent in the other CIP standards, for example, CIP-004-011. The obligation can be accomplished with one requirement, as follows. “The Responsible Entity shall implement one or more documented process(es) to mitigate the risk of the unauthorized disclosure or modification of Real-time Assessments and Real-time monitoring and control data while being transmitted between any Control Centers, except under CIP Exceptional Circumstances. This excludes oral communications. The process(es) shall identify: 1.1 security protection used to mitigate risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring and control data while being transmitted between Control Centers. 1.2 demarcation point(s) where security protection is applied for transmitting Real-time Assessment and Real-time monitoring and control data between Control Centers. Demarcation points identified by the Responsible Entity do not add additional Cyber Assets to the scope of the CIP Reliability Standards; and 1.3 roles and responsibilities of each Responsible Entity for applying security protection to the transmission of Real-time Assessment and Real-time monitoring and control data between Control Centers, when the Control Centers are owned or operated by different Responsible Entities.” This also includes important scoping from the implementation guidance that belongs in the requirement, that demarcation points don’t add additional Cyber Assets to the scope of the CIP standards. Also, the Proposed Reliability Standard lacks sufficient specificity (i.e., sufficient to stand on its own), without an endorsed Technical Rationale and Implementation Guidance. Relative to the draft Implementation Guidance document, MEC agrees with EEI that Industry will likely find it difficult to make any final judgments on the proposed Reliability Standard without NERC's endorsement of the draft Implementation Guidance. We trust that once the Proposed Reliability Standard gets closer to a final ballot NERC will endorse the final draft of the Implementation Guidance. In the event that doesn't occur, we fear the approval of this standard may be at risk.

Likes 0	
Dislikes 0	

Response

Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	
Comment	

N&ST believes that Figure 4 (“Network Diagram depicting communications through a 3rd party”) and its accompanying discussion describe a scenario for which CIP-012, as presently written, would not apply. As the figure is presently drawn, Control Centers “Alpha” and “Beta” are not communicating, that is, exchanging data, with each other. Each one is communicating with the “3rd party.” The fact that the 3rd party is presumably forwarding data t*hat it has processed in some fashion* to Beta after receiving it from Alpha, or vice-versa, does not, in N&ST’s opinion, constitute communications *between* two BES Control Centers.

If the SDT believes that communication links carrying Real-time Assessment data between BES Control Centers and 3rd party providers of such data, then CIP-012-1 should be modified to make this an explicit requirement.

Likes 0	
Dislikes 0	
Response	

Andrew Gallo - Austin Energy - 1,3,4,5,6	
Answer	No
Document Name	
Comment	

AE requests a formal definition of terms describing the data in question (*e.g.* “BES data” to address “monitoring” and “control” data types in a single definition. BES Data could be defined as, “Electronic data in BES Cyber Systems used to perform Supervisory Control and Data Acquisition (SCADA).” If the STD believes monitoring and control data should be defined separately, AE requests new NERC Glossary terms for “monitoring data” and “control data.”

Additionally, the Implementation Guidance states “The protection must also meet the security objective of mitigating the risk of unauthorized disclosure or modification of applicable data while in transit between Control Centers for the entire distance between CIP-012-1 demarcation points.” The document describes a situation where Entity Alpha exchanges data with Entity Beta through a “3rd party network.” The guidance asserts “a number of security controls may be leveraged such as network segmentation and system access control to protect the data as it transits the 3rd party network.” The document does not, however, describe the implications of the 3rd party circumventing those controls. Additionally, the controls in the 3rd party network do not address non-repudiation and, therefore, integrity as defined in NIST 800-53, Revision 4, page B-6. AE requests additional explanation to explain how the example approaches meet the security objective.

Although the SDT states it does not specify controls, the only examples provided include encryption. If other methods exist, the SDT should provide them.

Likes 0	

Dislikes 0	

Response

Janis Weddle - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Chelan PUD	
Answer	No
Document Name	

Comment
The Technical Rationale and Justification (TR&J) does not currently provide any technical implementation guidelines to identify where protections may be applied under the language of the CIP-012-1 standard. CHPD requests the addition of one or more sample connectivity drawings to the TR&J that depict compliant topology configurations showing the R1.1 security protection and R1.2 demarcation point placement that could be applied to an existing pair of in-scope Control Centers, including the associated BCS, ESP (EAP/EACMS), and PSP boundaries.

Likes 0	
Dislikes 0	

Response

David Francis - SRC & SWG - 2 - MRO,NPCC,SERC,RF, Group Name SRC + SWG	
Answer	Yes
Document Name	

Comment
Comments: There are concerns regarding the statement, “Demarcation points identified by the Responsible Entity do not add additional assets to the scope of the CIP Reliability Standards.” Entities may already include the demarcation points as Cyber Asset relevant to CIP-002 thru CIP-011. The statement could be revised as, “Demarcation points identified by the Responsible Entity is not intended to add additional assets to the scope of the CIP Reliability Standards.” With regards to the references models and narrative, it would be helpful to have the narrative and the reference model together. It is cumbersome to keep skipping back and forth in the document.

Likes 0	
Dislikes 0	

Response

Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	

Comment
Comments: There are concerns regarding the statement, “Demarcation points identified by the Responsible Entity do not add additional assets to the scope of the CIP Reliability Standards.” Entities may already include the demarcation points as Cyber Asset relevant to CIP-002 thru CIP-011. The statement could be revised as, “Demarcation points identified by the Responsible Entity are not intended to add additional assets to the scope of the CIP Reliability Standards.” With regards to the references models and narrative, it would be helpful to have the narrative and the reference model together. It is cumbersome to keep skipping back and forth in the document.

Likes 0	
Dislikes 0	

Response

Laurie Williams - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	Yes
Document Name	

Comment
While PNMR agrees with the example approaches in the draft Implementation Guidance there is one scenario that does not appear and possible should. Some entities use mailbox or virtual RTUs to communicate data between Control Centers either as redundant method to or in lieu of ICCP. Some Entities may forget that such communication could be in-scope of the standard especially if “Real-time Assessment and Real-time monitoring and control data” is passed through these mailbox or virtual RTUs. Typically these have points to point serial protocols and those serial connections would need to have protections applied. While PNMR does not know how many still use mailbox or virtual RTUs as an alternate means, it is something the drafting team should take into consideration.

Likes 0	
Dislikes 0	

Response

Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE	
Answer	Yes
Document Name	

Comment
Xcel Energy agrees that the approaches offered in the CIP-012-2 Implementation Guidance are non-prescriptive and can be sufficient models to be used in implementation. However, Xcel Energy cannot agree with the proposed timeline of 24 months. We share real-time data with Registered Entities (REs) such as the Reliability Coordinators (RCs) including MISO, SPP and PEAK. Additionally, we would share data with many utilities with Control Centers across our service territory. Finding a common technological solution to implement the proposed mitigating activities in the

Requirements will take a substantial effort on the part of all REs. Once a common technology and all legal agreements between REs are in place, Xcel Energy may still have to purchase and implement those technology solutions.

Xcel Energy stakeholders suggest that NERC should advice and work with all RCs to agree upon a common technology first and then drive those solutions from the RC down to each utility in scope.

Likes 0	
Dislikes 0	

Response

Chris Scanlon - Exelon - 1,3,5,6

Answer	Yes
Document Name	

Comment

Exelon generally agrees with the approach in the draft Implementation Guidance, noting the following concerns and suggestions.

1. We have a concern that the CIP-012-1 Standard may be approved prior to NERC endorsement of the Technical Rationale and Justification and the Implementation Guidance for CIP-012. Our approval of the CIP-012-1 Standard language as presented is in part predicated upon the clarifications present within the Implementation Guidance. We would expect to see the endorsement by NERC of these supporting documents before we vote for final approval of the Standard.

2. Within the Standard, Technical Rationale and Justification, and the Implementation Guidance, there is no mention of the scenario of data transmission between a Control Center and its associated Data Center(s) located in separate physical locations. Clarification of whether this intra-Control Center data transmission is in scope seems appropriate.

3. Our SMEs raised questions about data not currently determined to have a 15-minute impact and therefore out of scope for CIP-002 thru CIP-011, e.g. synchrophasers data. Can we automatically assume then, that this same data is also currently out of scope for CIP-012? Looking for clarification on this question within the Standard or supporting documents.

Likes 0	
Dislikes 0	

Response

Eleanor Ewry - Puget Sound Energy, Inc. - 1,3,5

Answer	Yes
Document Name	

Comment

Further details about the technological controls required to meet the requirements would be helpful. Providing additional, specific examples about appropriate approaches would help ensure entities implement sufficient protection mechanisms, per the requirements.

Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	Yes
Document Name	
Comment	
The California ISO supports the comments of the IRC Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Page 1 Introduction - Recommend including in the Introduction the same paragraph found in the Technical Rationale and Justification Introduction as it provides an important perspective that appears to not be fully understood. *'Although the Commission directed NERC to develop modifications to CIP-006, the SDT determined that modifications to CIP-006 would not be appropriate. There are differences between the plan(s) required to be developed and implemented for CIP-012-1 and the protection required in CIP-006-6 Requirement R1 Part 1.10. CIP-012-1 Requirements R1 and R2 protect the applicable data during transmission between two separate Control Centers. CIP-006 Requirement R1 Part 1.10 protects nonprogrammable communication components within an Electronic Security Perimeter (ESP) but outside of a Physical Security Perimeter (PSP). The transmission of applicable data between Control Centers takes place outside of an ESP. Therefore, the protection contained in CIP-006-6 Requirement R1 Part 1.10 does not apply.*'	
Likes 0	
Dislikes 0	
Response	
John Tolo - Unisource - Tucson Electric Power Co. - 1	
Answer	Yes
Document Name	

Comment
Sometimes the lack of specifics causes confusion and lost time. Being more specific about the technological controls would be more helpful. For instance, PCI-DSS specifically calls out when encryption is needed for data at-rest and in-transit. If the intent is to encrypt data, it would be better to say so up-front and specify the protection boundaries. Some entities may decide to implement different protection mechanisms that may not be sufficient from a security perspective and then through the course of presentations and guidance have to re-work. TEP appreciates the opportunity to comment.

Likes 0	
Dislikes 0	

Response

Brandon Cain - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - FRCC,MRO,WECC,Texas RE,SERC,SPP RE	
Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion and ISO-NE	
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	
David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	Yes
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	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	

Texas RE has the following comments regarding the implementation guidance:

In the Identification of Security Protection section on page 6: "*Alternatively, a Responsible Entity* may *demonstrate implementation through* ***monitoring*** *of the security control such as a report generated from an automated tool that* ***monitors*** *the encryption service used to protect a communications link*."

- Texas RE recommends adding monitoring **and logging**, monitors **and logs**.

In the Reference Model Discussion for Requirement R1 section on page 7:

"*Additionally, Entity Alpha does not need to consider any communications to other non-Control Center facilities such as generating plants or substations. These communications are out of scope for CIP-012-1*."

- Although this may be out-of-scope as a best security practice, Texas RE recommend Entity Alpha should "*consider any communications to other non-Control Center facilities such as generating plants or substations*."

In the Identification of Security Protection section on page 13:

"*When physical security controls are used, Entity Alpha* ***may*** *demonstrate the implementation of physical protection* ***using a floorplan diagram*** *showing the physical access controls in place*."

- Texas RE suggests including other types of evidence with a floorplan as a floorplan diagram alone would not be sufficient.

Likes 0	
Dislikes 0	
Response	

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Project 2016-02

Modifications to CIP Standards

Consideration of Comments Regarding Implementation Guidance and Technical Rationale and Justification for CIP-012

March 2018

RELIABILITY | ACCOUNTABILITY

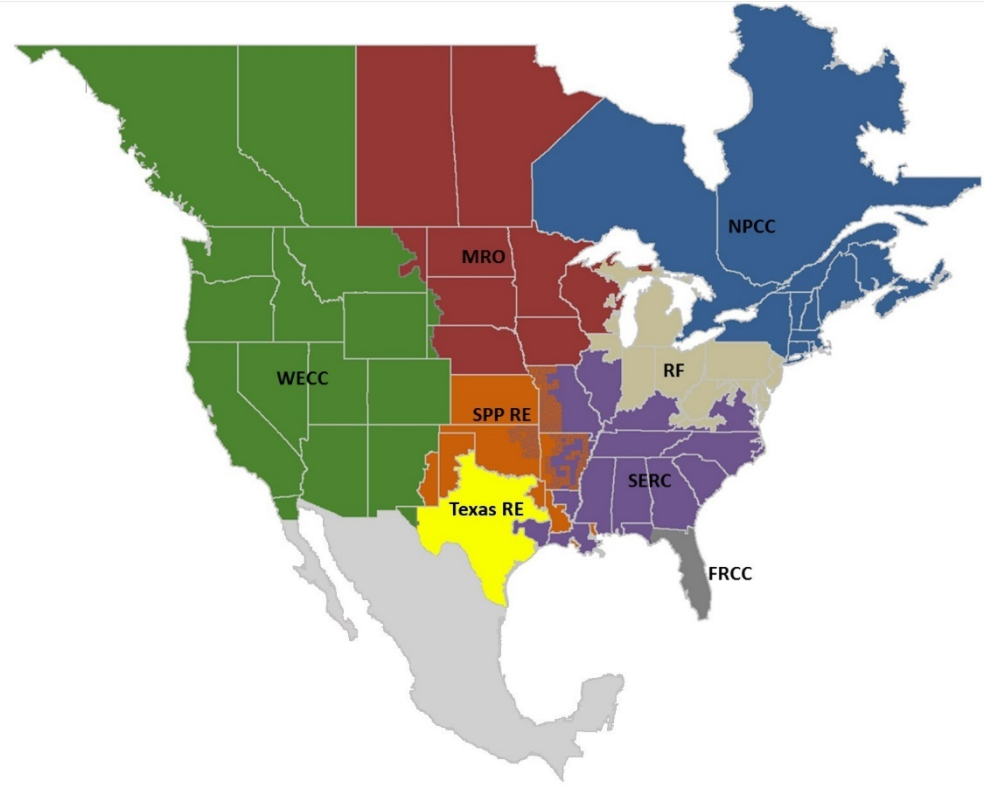



3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Preface

The North American Electric Reliability Corporation (NERC) is a not-for-profit international regulatory authority whose mission is to assure the reliability and security of the bulk power system (BPS) in North America. NERC develops and enforces Reliability Standards; annually assesses seasonal and long-term reliability; monitors the BPS through system awareness; and educates, trains, and certifies industry personnel. NERC's area of responsibility spans the continental United States, Canada, and the northern portion of Baja California, Mexico. NERC is the Electric Reliability Organization (ERO) for North America, subject to oversight by the Federal Energy Regulatory Commission (FERC) and governmental authorities in Canada. NERC's jurisdiction includes users, owners, and operators of the BPS, which serves more than 334 million people.

The North American BPS is divided into eight Regional Entity (RE) boundaries as shown in the map and corresponding table below.



The North American BPS is divided into eight RE boundaries. The highlighted areas denote overlap as some load-serving entities participate in one Region while associated transmission owners/operators participate in another.

FRCC	Florida Reliability Coordinating Council
MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
SPP RE	Southwest Power Pool Regional Entity
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

The standard drafting team (SDT) appreciates industry comments on the proposed Implementation Guidance and Technical Rationale and Justification for CIP-012. The SDT considered the comments submitted during the posting of the proposed Implementation Guidance and Technical Rationale and Justification for CIP-012, and adapted its revision approach for the second proposal currently posted. Additionally, the SDT conducted substantial outreach during the revision process, through in-person meetings, conference calls, and stakeholder organization presentations.

On January 21, 2016, the Federal Energy Regulatory Commission (FERC) issued Order No. 822 Revised Critical Infrastructure Protection Reliability Standards. In this order, FERC approved revisions to version 5 of the CIP standards.

Response to Comments

The SDT has carefully reviewed each stakeholder comment and has revised language where suggested changes are consistent with SDT intent and industry consensus. The SDT reviewed and responded to each comment in summary form below.

There were 30 sets of comments, comprised of approximately 84 different people across approximately 59 companies representing 10 of the Industry Segments.

All comments submitted can be reviewed in their original format on the project page.

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process. If you feel there has been an error or omission, you can contact the Senior Director of Standards, Howard Gugel (via email) or at (404) 446-9693.

Consideration of Comments – Summary Responses

Implementation Guidance

- Commenters recommended creating a new "BES data" NERC Glossary term to be used to clearly scope the data in question. Commenters also recommended defining the terms "monitoring data" and "control data" in the NERC Glossary.

  The SDT asserts that Real-time monitoring is a well-understood concept that is included in the TOP and IRO standards. Additionally, Real-time Assessment is a defined term within the NERC Glossary of Terms Used in Reliability Standards. Creating new terms and definitions could cause unintended impacts on other standards. The SDT removed "and control" from Requirement R1 and from the Technical Rationale.

- A commenter noted the Technical Rationale and Justification document does not provide any technical implementation guidelines to identify where protections may be applied under the language of the CIP-012-1 standard. The commenter also requested the addition of one or more sample connectivity drawings to the Technical Rationale and Justification document that depict compliant topology configurations showing the R1.1 security protection and R1.2 demarcation point placement that could be applied to an existing pair of in-scope Control Centers, including the associated BCS, ESP (EAP/EACMS), and PSP boundaries.

  The Technical Rationale and Justification document explains the technical rationale for the proposed Reliability Standard. This Technical Rationale and Justification document does not provide examples of how to implement the requirements. However, the SDT has identified physically secure areas and ESP firewalls in the diagrams in the Implementation Guidance for CIP-012-1.

- A commenter recommended the following paragraph from the Technical Rationale and Justification Introduction as it provides an important perspective that appears to not be fully understood. *"Although the Commission directed NERC to develop modifications to CIP-006, the SDT determined that modifications to CIP-006 would not be appropriate. There are differences between the plan(s) required to be developed and implemented for CIP-012-1 and the protection required in CIP-006-6 Requirement R1 Part 1.10. CIP-012-1 Requirements R1 and R2 protect the applicable data during transmission between two separate Control Centers. CIP-006 Requirement R1 Part 1.10 protects nonprogrammable communication components within an Electronic Security Perimeter (ESP) but outside of a Physical Security Perimeter (PSP). The transmission of applicable data between Control Centers takes place outside of an ESP. Therefore, the protection contained in CIP-006-6 Requirement R1 Part 1.10 does not apply.*"

  The SDT notes this paragraph is an explanation of the rationale behind developing CIP-012. It does not include information on examples of implementation. The SDT has declined to add this to the Implementation Guidance for these reasons.

- A commenter recommended adding logging to the Identification of Security Protection section on page 7. The commenter also recommended that entities should consider any communications to other non-Control Center facilities such as generating plants or substations. The commenter also suggests including other types of evidence with a floorplan as a floorplan diagram alone would not be sufficient.

  The SDT thanks you for the comments. The SDT notes that the Implementation Guidance is providing a small set of examples of implementation and has aligned the content to the requirement language only. It is not the intent of the SDT to add more rigor in meeting best practice that may be outside the scope of the requirement language. The SDT notes that additional Implementation Guidance documents can be drafted

for any standard. Individual entities are encouraged to work with pre-qualified organizations to submit additional Implementation Guidance for consideration of endorsement by the ERO.

- Commenters requested more examples of technical controls, noting that lack of specifics can cause confusion and lost time. This will aid entities who may decide to implement protection mechanisms that may not be sufficient from a security perspective and then through the course of presentations and guidance have to re-work.

  The SDT thanks you for the comments. The SDT notes that the Implementation Guidance is providing a small set of examples of implementation. SDT notes that additional Implementation Guidance documents can be drafted for any standard. Individual entities are encouraged to work with pre-qualified organizations to submit additional Implementation Guidance for consideration of endorsement by the ERO.

- Commenters noted the Implementation Guidance for CIP-012 does not address non-repudiation and, therefore, integrity as defined by NIST 800-53, Revision 4, page B-6. The commenter requests that the SDT provide additional implementation guidance regarding how the protections are required "…in a manner that reflects the risks posed to bulk electric system reliability," as stated on page 12 of FERC Order No. 822.

  The SDT thanks you for the comments and has removed the example from the Implementation Guidance document.

- Commenters requested that the SDT consider consolidating Requirement R2 into Requirement R1, noting it is unnecessary to have two requirements.

  The SDT agrees with comments regarding a single requirement and has modified Requirement R1 and updated the Implementation Guidance accordingly.

- A commenter noted concerns related to mailbox or virtual RTUs used to communicate data between Control Centers as a redundant method to, or in lieu, of ICCP. Some Entities may forget that such communication could be in-scope of the standard especially if Real-time Assessment and Real-time monitoring and control data is passed through these mailbox or virtual RTUs.

  The SDT thanks you for the comments. As plans are developed, entities should be aware of the various means that data is communicated between Control Centers and account for those means in the plan document(s). The SDT notes that the Implementation Guidance is providing a small set of examples of implementation. SDT notes that additional Implementation Guidance documents can be drafted for any standard. Individual entities are encouraged to work with pre-qualified organizations to submit additional Implementation Guidance for consideration of endorsement by the ERO.

- A commenter noted concerns with the inclusion of "and control" in Requirement R1 and the Implementation Guidance. They also questioned the need to identify roles and responsibilities for applying security protections. They disagreed with including response in considering roles and responsibilities. They also disagreed with specifying an encryption example (AES-128). They also recommended including guidance on agreements with third parties handling data.

  The SDT thanks you for the comments. The SDT notes that the Implementation Guidance is providing a small set of examples of implementation. The SDT intended to provide some specific examples to aid entities. Based on comments, the SDT removed "and control" and "roles" from Requirement R1 and the Implementation Guidance. The SDT contends is it is necessary to document the responsibilities when

communication between Control Centers involves more than one entity and has left "responsibilities" in Requirement R1 and the Implementation Guidance. The SDT removed the specific encryption example from the Implementation Guidance. The SDT removed the example related to third parties from the Implementation Guidance.

- A commenter requested ERO endorsement of the Implementation Guidance before final ballot on CIP-012.

  The SDT thanks you for the comment. The SDT is actively working with NERC staff to coordinate and gain endorsement of the guidance in a timely manner.

- One commenter noted a question of whether communication between a Control Center and associated data centers would be in scope for CIP-012.

  The SDT developed CIP-012 in response to FERC Order 822. Paragraph 58 of FERC Order 822 notes that the requirement "should encompass communication links and data for intra-Control Center and inter-Control Center communications." Through discussions with FERC staff, the SDT came to understand that this paragraph was intended to convey that the requirement should include communications between Control Centers operated by a single entity (such as between a primary and backup Control Center) and communications between Control Centers operated by neighboring entities (such as between a TOP and its RC). The SDT notes that the Control Center by definition includes the associated data center and should, therefore be included with protecting intra-Control Center communications. The SDT did not specify protection for communication within a single Control Center as it did not intend to interfere or cause unintended consequences with the inter-process communications that enable an EMS to function properly.

- A commenter raised questions about data not currently determined to have a 15-minute impact and therefore out of scope for CIP-002 thru CIP-011, e.g. synchrophasers data. The question if this data is out of scope for CIP-012.

  CIP-012 does not use the reference to 15-minute impact. If the data in question is used for Real-time Assessment or Real-time monitoring, the data is in scope for CIP-012.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the third draft of the proposed standard.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23 - April 21, 2016
SAR posted for comment	June 1 – June 30, 2016
Informal comment period	February 10- March 13, 2017
45-day formal comment period with initial ballot	July 27 – September 11, 2017
45-day formal comment period with additional ballot	October 27 – December 11, 2017
45-day formal comment period with additional ballot	March 16 – April 30, 2018

Anticipated Actions	Date
45-day formal comment period with additional ballot	May 18 – July 2, 2018
10-day final ballot	July 30 – August 8, 2018
NERC Board	August 16, 2018

A. Introduction

1. **Title:** Cyber Security – Communications between Control Centers

2. **Number:** CIP-012-1

3. **Purpose:** To protect the confidentiality and integrity of Real-time Assessment and Real-time monitoring data transmitted between Control Centers.

4. **Applicability:**

   4.1. Functional Entities: The requirements in this standard apply to the following functional entities, referred to as "Responsible Entities," that own or operate a Control Center.

   4.1.1. Balancing Authority

   4.1.2. Generator Operator

   4.1.3. Generator Owner

   4.1.4. Reliability Coordinator

   4.1.5. Transmission Operator

   4.1.6. Transmission Owner

   4.2. Exemptions: The following are exempt from Reliability Standard CIP-012-1:

   4.2.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

   4.2.2. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

5. **Effective Date:** See Implementation Plan for CIP-012-1.

B. Requirements and Measures

R1. The Responsible Entity shall implement one or more documented plan(s) to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring data while being transmitted between any Control Centers. This requirement excludes oral communications. The plan shall include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. Identification of security protection used to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers;

1.2. Identification of where the Responsible Entity applied security protection for transmitting Real-time Assessment and Real-time monitoring data between Control Centers; and

1.3. If the Control Centers are owned or operated by different Responsible Entities, identify the responsibilities of each Responsible Entity for applying security protection to the transmission of Real-time Assessment and Real-time monitoring data between those Control Centers.

M1. Evidence may include, but is not limited to, documented plan(s) that meet the security objective of Requirement R1 and documentation demonstrating the implementation of the plan(s).

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" (CEA) means NERC, the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

- The Responsible Entities shall keep data or evidence of each Requirement in this Reliability Standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	N/A	The Responsible Entity documented its plan(s) but failed to include one of the applicable parts of the plan as specified in Requirement R1.	The Responsible Entity documented its plan(s) but failed to include two of the applicable parts of the plan as specified in Requirement R1.	The Responsible Entity failed to document plan(s) for Requirement R1; Or The Responsible Entity failed to implement any Part of its plan(s) for Requirement R1, except under CIP Exceptional Circumstances.

D. Regional Variances

None.

E. Associated Documents

Implementation Plan.

Version History

Version	Date	Action	Change Tracking
1	TBD	Respond to FERC Order No. 822	N/A

Standard Attachments

None.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the ~~second~~ third draft of the proposed standard.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23 - April 21, 2016
SAR posted for comment	June 1 – June 30, 2016
Informal comment period	February 10- March 13, 2017
45-day formal comment period with ~~additional~~ initial ballot	July 27 – September 11, 2017
45-day formal comment period with additional ballot	October 27 – December 11, 2017
45-day formal comment period with additional ballot	~~TBD~~March 16 – April 30, 2018

Anticipated Actions	Date
45-day formal comment period with additional ballot	May 18 – July 2, 2018
10-day final ballot	~~TBD~~July 30 – August 8, 2018
NERC Board	~~TBD~~August 16, 2018

A. Introduction

1. **Title:** Cyber Security – Communications between Control Centers

2. **Number:** CIP-012-1

3. **Purpose:** To protect the confidentiality and integrity of Real-time Assessment and Real-time monitoring ~~and control~~ data transmitted between Control Centers.

4. **Applicability:**

   4.1. Functional Entities: The requirements in this standard apply to the following functional entities, referred to as "Responsible Entities," that own or operate a Control Center.

   4.1.1. Balancing Authority

   4.1.2. Generator Operator

   4.1.3. Generator Owner

   4.1.4. Reliability Coordinator

   4.1.5. Transmission Operator

   4.1.6. Transmission Owner

   4.2. Exemptions: The following are exempt from Reliability Standard CIP-012-1:

   4.2.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

   4.2.2. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

5. **Effective Date:** See Implementation Plan for CIP-012-1.

B. Requirements and Measures

R1. The Responsible Entity shall implement one or more documented plan(s) to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring ~~and control~~ data while being transmitted between any Control Centers. This requirement excludes oral communications. The plan shall include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. Identification of security protection used to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring ~~and control~~ data while being transmitted between Control Centers;

1.2. Identification of ~~demarcation point(s)~~ where the Responsible Entity applied security protection ~~is applied~~ for transmitting Real-time Assessment and Real-time monitoring ~~and control~~ data between Control Centers; and

1.3. If ~~Identification of roles and responsibilities of each Responsible Entity for applying security protection to the transmission of Real-time Assessment and Real-time monitoring and control data between Control Centers, when~~ the Control Centers are owned or operated by different Responsible Entities, ~~:~~ ~~I~~identify the responsibilities of each Responsible Entity for applying security protection to the transmission of Real-time Assessment and Real-time monitoring data between those Control Centers.

M1. Evidence may include, but is not limited to, documented plan(s) that meet the security objective of Requirement R1~~.~~ and documentation demonstrating the implementation of the plan(s).

~~**R2.** The Responsible Entity shall implement the plan(s) specified in Requirement R1, except under CIP Exceptional Circumstances.~~

~~**M2.** Evidence may include, but is not limited to, documentation demonstrating implementation of the plans developed pursuant to Requirement R1.~~

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" (CEA) means NERC, the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

- The Responsible Entities shall keep data or evidence of each Requirement in this Reliability Standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.

- The Compliance Enforcement Authority ~~(CEA)~~ shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	N/A	The Responsible Entity documented its plan(s) but failed to include one of the applicable parts of the plan as specified in Requirement R1.	The Responsible Entity documented its plan(s) but failed to include two of the applicable parts of the plan as specified in Requirement R1.	The Responsible Entity failed to document plan(s) for Requirement R1;. Or The Responsible Entity failed to implement any Part of its plan(s) for Requirement R1, except under CIP Exceptional Circumstances.
~~**R2.**~~	~~N/A~~	~~N/A~~	~~N/A~~	~~The Responsible Entity failed to implement its plan(s) as specified in Requirement R1, except under CIP Exceptional Circumstances.~~

D. Regional Variances

None.

E. Associated Documents

Implementation Plan.

Version History

Version	Date	Action	Change Tracking
1	TBD	Respond to FERC Order No. 822	N/A

Standard Attachments

None.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2016-02 Modifications to CIP Standards
Reliability Standard CIP-012-1

Applicable Standard

- Reliability Standard CIP-012-1 - Cyber Security – Communications between Control Centers

Requested Retirements

- None

Prerequisite Standard

These standard(s) or definitions must be approved before the Applicable Standard becomes effective:

- None

Applicable Entities

- Balancing Authority
- Generator Operator
- Generator Owner
- Reliability Coordinator
- Transmission Operator
- Transmission Owner

Effective Date

Reliability Standard CIP-012-1 - Cyber Security – Communications between Control Centers

Where approval by an applicable governmental authority is required, Reliability Standard CIP-012-1 shall become effective on the first day of the first calendar quarter that is twenty-four (24) calendar months after the effective date of the applicable governmental authority's order approving the standard, or as otherwise provided for by the applicable governmental authority.

Where approval by an applicable governmental authority is not required, Reliability Standard CIP-012-1 shall become effective on the first day of the first calendar quarter that is twenty-four (24) calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Comment Form

Project 2016-02 Modifications to CIP Standards
CIP-012-1

Do not use this form for submitting comments. Use the Standards Balloting and Commenting System (SBS) to submit comments on **CIP-012-1 – Cyber Security – Communications between Control Centers.** Comments must be submitted by **8 p.m. Eastern, Monday, April 30, 2018.**

Additional information is available on the project page. If you have questions, contact Jordan Mallory at (404) 446-2589 or Mat Bunch at (404) 446-9785.

Background Information

On January 21, 2016, the Commission issued Order No. 822, approving seven CIP Reliability Standards and new or modified definitions, and directing modifications to the CIP Reliability Standards. Among others, the Commission directed NERC to "develop modifications to the CIP Reliability Standards to require responsible entities to implement controls to protect, at a minimum, communication links and sensitive bulk electric system data communicated between bulk electric system Control Centers in a manner that is appropriately tailored to address the risks posed to the bulk electric system by the assets being protected (i.e., high, medium, or low impact)." (Order 822, Paragraph 53)

The Project 2016-02 Standard Drafting Team (SDT) drafted Reliability Standard CIP-012-1 to require Responsible Entities to implement controls to protect sensitive Bulk Electric System (BES) data while being transmitted over communications links between BES Control Centers. Due to the sensitivity of the data being communicated between the Control Centers, the standard applies to all impact levels (i.e., high, medium, or low impact).

The SDT drafted CIP-012-1 allowing Responsible Entities to apply protection to the links, the data, or both, in order to satisfy the security objective consistent with the capabilities of the Responsible Entity's operational environment. Requirement R1 requires Responsible Entities to implement one or more document plans that protect Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers. The plan(s) must address how the Responsible Entity will mitigate the risk of unauthorized disclosure or modification of the applicable data.

Questions

1. Requirement R1: The SDT drafted CIP-012-1 Requirement R1 for the Responsible Entity to implement one or more documented plan(s) to mitigate the risk of the unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring data while being transmitted between any Control Centers. Do you agree with this revision? If not, please provide the basis for your disagreement and an alternate proposal.

   ☐ Yes
   ☐ No

   Comments:

2. Implementation Plan: The SDT established the Implementation Plan to make the standard effective the first day of the first calendar quarter that is twenty-four (24) calendar months after the effective date of the applicable governmental authority's order approving the standard, or as otherwise provided for by the applicable governmental authority. Do you agree with this proposal? If you think an alternate implementation time period is needed, please provide a detailed explanation of actions and time needed to meet the implementation deadline.

   ☐ Yes
   ☐ No

   Comments:

3. The SDT modified the draft Technical Rationale and Justification for CIP-012 to assist in understanding the technology and technical requirements in the Reliability Standard. It also contains information on the SDT's intent in drafting the requirements. Do you agree with the technology and technical requirements in the draft Technical Rationale and Justification? If you do not agree, or if you agree but have comments or suggestions for the draft Technical Rationale and Justification, please provide your recommendation and explanation.

   ☐ Yes
   ☐ No

   Comments:

4. The SDT modified the draft Implementation Guidance for CIP-012 to provide examples of how a Responsible Entity could comply with the requirements. The draft Implementation Guidance does not prescribe the only approach to compliance. Rather, it describes what the SDT believes would be effective ways to comply with the standard. See NERC's Compliance Guidance policy for information on Implementation Guidance. Do you agree with the draft Implementation Guidance?

If you do not agree, or if you agree but have comments or suggestions for the draft Implementation Guidance, please provide your recommendation and explanation.

☐ Yes
☐ No

Comments:

5. The SDT believes proposed CIP-012-1 provides entities with flexibility to meet the reliability objectives in a cost effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost effective approaches, please provide your recommendation and, if appropriate, technical justification.

☐ Yes
☐ No

Comments:

Project 2016-02 Consideration of Issues and Directives

Federal Energy Regulatory Commission Order No. 822

March 2018

Directives from FERC Order No. 822		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
53	53. As discussed in detail below, however, the Commission concludes that modifications to CIP-006-6 to provide controls to protect, at a minimum, communication links and data communicated between bulk electric system Control Centers are necessary in light of the critical role Control Center communications play in maintaining bulk electric system reliability. Therefore, we adopt the NOPR proposal and direct that NERC, pursuant to section 215(d)(5) of the FPA, develop modifications to the CIP Reliability Standards to require responsible entities to implement controls to protect, at a minimum, communication links and sensitive bulk electric system data communicated between bulk electric system Control Centers in a manner that is appropriately tailored to address the risks posed to the bulk electric system by the assets being protected (i.e., high, medium, or low impact).	The Project 2016-02 Standard Drafting Team (SDT) drafted Reliability Standard CIP-012-1 Requirement R1 to require responsible entities to implement one or more documented plan(s) to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring data while being transmitted between Bulk Electric System (BES) Control Centers. Due to the sensitivity of the data being transmitted between the Control Centers, the SDT created the standard to apply to all impact levels of BES Cyber Systems (i.e., high, medium, or low impact). Based on operational risk, the SDT determined that Real-time Assessments and Real-time monitoring data was the appropriate scope of the requirement. This critical information is necessary for immediate situational awareness and real-time operation of the BES. The SDT has drafted the requirement allowing Responsible Entities the flexibility to apply protection to the

Directives from FERC Order No. 822		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
		communication links, the data, or both, consistent with their operational environments to satisfy the security objective of the Commission's directive FERC Order No. 822 specifically references CIP-006-6, which pertains to physical security controls. CIP-006-6, Requirement R1, Part 1.10 focuses on protecting the nonprogrammable communication components between Cyber Assets within the same ESP for medium and high impact BES Cyber Systems. The SDT asserts that most of the communications contemplated by FERC Order No. 822 are not within the same ESP, and, as such, CIP-006-6, Requirement R1, Part 1.10 would not be the appropriate location for this requirement.
54	54. NERC and other commenters recognize that inter-Control Center communications play a critical role in maintaining bulk electric system reliability by, among other things, helping to maintain situational awareness and reliable bulk electric system operations through timely and accurate communication between Control Centers.[59] We agree with this assessment. In order for certain responsible entities such as reliability coordinators, balancing authorities, and transmission operators to adequately perform their reliability functions, their associated control centers must be capable of receiving and storing a variety of sensitive	The SDT agrees that inter-Control Center communications play a critical role in Bulk Electric System reliability. Responsible Entities should therefore apply security measures to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring data. Since the current CIP Reliability Standards do not address this, the SDT has designed the requirement to protect the data while it is being transmitted between inter-entity and intra-entity Control Centers. The SDT has drafted a requirement that allows responsible entities to apply protection to the communication links, the

Directives from FERC Order No. 822		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
	bulk electric system data from interconnected entities. Accordingly, we find that additional measures to protect both the integrity and availability of sensitive bulk electric system data are warranted.[60] We also understand that the attributes of the data managed by responsible entities could require different information protection controls. [61] For instance, certain types of reliability data will be sensitive to data manipulation type attacks, while other types of reliability data will be sensitive to eavesdropping type attacks aimed at collecting operational information (such as line and equipment ratings and impedances). NERC should consider the differing attributes of bulk electric system data as it assesses the development of appropriate controls. Footnotes: [59] NERC Comments at 20. [60] Protecting the integrity of bulk electric system data involves maintaining and ensuring the accuracy and consistency of inter-Control Center communications. Protecting the availability of bulk electric system data involves ensuring that required data is available when needed for bulk electric system operations.	data, or both to satisfy the security objective consistent with the capabilities of the responsible entity's operational environment.

Directives from FERC Order No. 822		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
	[61] Moreover, in order for certain responsible entities to adequately perform their Reliability Functions, the associated control centers must be capable of receiving and storing a variety of sensitive data as specified by the IRO and TOP Standards. For instance, pursuant to Reliability Standard TOP-003-3, Requirements R1, R3 and R5, a transmission operator must maintain a documented specification for data and distribute its data specification to entities that have data required by the transmission operator's Operational Planning Analyses, Real-time Monitoring and Real-time Assessments. Entities receiving a data specification must satisfy the obligation of the documented specification.	
55	55. With regard to NERC's development of modifications responsive to our directive, we agree with NERC and other commenters that NERC should have flexibility in the manner in which it addresses the Commission's directive. Likewise, we find reasonable the principles outlined by NERC that protections for communication links and sensitive bulk electric system data communicated between bulk electric system Control Centers: (1) should not have an adverse effect on reliability, including the recognition of instances where the introduction of latency could have negative results; (2) should account for the risk levels of assets and	The SDT drafted Reliability Standard CIP-012-1 to mitigate the risk of unauthorized disclosure or modification of Real-time Assessments and Real-time monitoring data while being transmitted between Control Centers. The SDT developed and objective-based rather than prescriptive requirement. This approach will allow Responsible Entities flexibility in protecting these communications networks and sensitive BES data in a manner suited to each of their respective operational environments. It will also allow Responsible Entities to implement protection that considers the risks noted by the Commission. The SDT identified a need to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment

Directives from FERC Order No. 822		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
	information being protected, and require protections that are commensurate with the risks presented; and (3) should be results-based in order to provide flexibility to account for the range of technologies and entities involved in bulk electric system communications.[62] Footnote: [62] See NERC Comments at 20-21.	and Real-time monitoring data regardless of asset risk level. The proposal requires protection for all Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers.
56	56. We disagree with the assertion of NIPSCO and G&T Cooperatives that the risk posed by bulk electric system communication networks does not justify the costs of implementing controls. Communications between Control Centers over such networks are fundamental to the operations of the bulk electric system, and the record here does not persuade us that controls for such networks are not available at a reasonable cost (through encryption or otherwise). Nonetheless, we recognize that not all communication network components and data pose the same risk to bulk electric system reliability and may not require the same level of protection. We expect NERC to develop controls that reflect the risk posed by the asset or data being protected, and that can be implemented in a reasonable manner. It is important to recognize that certain entities are already required to exchange	The SDT noted the FERC reference to additional Reliability Standards (TOP-003-3 and IRO-010-2) and the responsibilities to protect the data in accordance with those standards. The SDT interpreted these references as examples of potentially sensitive BES data and chose to base the CIP-012 requirements on the data specifications in TOP-003-3 and IRO-010-2. This consolidates scoping and helps ensure that Responsible Entities mitigate the risk of the unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring data, rather than leaving the scoping of sensitive bulk electric system data to individual Responsible Entities. The SDT drafted CIP-012-1 to address confidentiality and integrity of Real-time Assessment and Real-time monitoring data. This was accomplished by drafting the requirement to mitigate the risk from unauthorized disclosure or modification. The SDT asserts that the availability of this data is already

Directives from FERC Order No. 822		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
	necessary real-time and operational planning data through secured networks using a "mutually agreeable security protocol," regardless of the entity's size or impact level.[63] 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. Footnote: [63] See Reliability Standards TOP-003-3, Requirement R5 and IRO-010-2, Requirement R3.	required by the performance obligation of the TOP and IRO Reliability Standards. The SDT drafted CIP-012-1 to address the data while being transmitted. The SDT contends that this data is maintained within BES Cyber Systems, and is afforded the protections of CIP-003 through CIP-011 while at rest.
58	58. Several commenters sought clarification whether Control Centers owned by multiple registered entities would be included under the Commission's proposal. We clarify that the scope of the directed modifications apply to Control Center communications from facilities at all impact levels, regardless of ownership. The directed modification should encompass communication links and data for intra-Control Center and inter-Control Center communications.	The SDT drafted CIP-012-1 to apply to all impact levels of BES Cyber Systems (i.e., high, medium, or low impact), regardless of ownership. The SDT designed the requirement to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring data while being transmitted between inter-entity and intra-entity BES Control Centers.

Directives from FERC Order No. 822		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
62	62. Several commenters addressed encryption and latency. Based on the record in this proceeding, it is reasonable to conclude that any lag in communication speed resulting from implementation of protections should only be measureable on the order of milliseconds and, therefore, will not adversely impact Control Center communications. Several commenters raise possible technical implementation difficulties with integrating encryption technologies into their current communications networks. Such technical issues should be considered by the standard drafting team when developing modifications in response to this directive, and may be resolved, e.g., by making certain aspects of the revised CIP Standards eligible for Technical Feasibility Exceptions.	The SDT developed an objective-based rather than prescriptive requirement. This approach will allow Responsible Entities flexibility in mitigating the risk of unauthorized disclosure or modification of Real-time Assessments and Real-time monitoring data in a manner suited to each of their respective operational environments. It will also allow Responsible Entities to implement protection that considers the risks noted by the Commission.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Project 2016-02 Consideration of Issues and Directives

Federal Energy Regulatory Commission Order No. 822

~~October 27~~March~~,~~ 201~~8~~7~~

Directives from FERC Order No. 822		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
53	53. As discussed in detail below, however, the Commission concludes that modifications to CIP-006-6 to provide controls to protect, at a minimum, communication links and data communicated between bulk electric system Control Centers are necessary in light of the critical role Control Center communications play in maintaining bulk electric system reliability. Therefore, we adopt the NOPR proposal and direct that NERC, pursuant to section 215(d)(5) of the FPA, develop modifications to the CIP Reliability Standards to require responsible entities to implement controls to protect, at a minimum, communication links and sensitive bulk electric system data communicated between bulk electric system Control Centers in a manner that is appropriately tailored to address the risks posed to the bulk electric system by the assets being protected (i.e., high, medium, or low impact).	The Project 2016-02 Standard Drafting Team (SDT) drafted Reliability Standard CIP-012-1 Requirement R1 to require responsible entities to implement ~~document~~ one or more documented plan(s) to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring ~~and control~~ data while being transmitted between Bulk Electric System (BES) Control Centers. ~~Requirement R2 requires implementation of the documented plan(s).~~ Due to the sensitivity of the data being transmitted between the Control Centers, the SDT created the standard to apply to all impact levels of BES Cyber Systems (i.e., high, medium, or low impact). Based on operational risk, the SDT determined that Real-time Assessments and Real-time monitoring ~~and control~~ data was the appropriate scope of the requirement. This critical information is necessary for immediate situational awareness and real-time operation of the BES.

Directives from FERC Order No. 822		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
		The SDT has drafted ~~requirements~~ the requirement allowing Responsible Entities the flexibility to apply protection to the communication links, the data, or both, consistent with their operational environments to satisfy the security objective of the Commission's directive FERC Order No. 822 specifically references CIP-006-6, which pertains to physical security controls. CIP-006-6, Requirement R1, Part 1.10 focuses on protecting the nonprogrammable communication components between Cyber Assets within the same ESP for medium and high impact BES Cyber Systems. The SDT asserts that most of the communications contemplated by FERC Order No. 822 are not within the same ESP, and, as such, CIP-006-6, Requirement R1, Part 1.10 would not be the appropriate location for this requirement.
54	54. NERC and other commenters recognize that inter-Control Center communications play a critical role in maintaining bulk electric system reliability by, among other things, helping to maintain situational awareness and reliable bulk electric system operations through timely and accurate communication between Control Centers.[59] We agree with this assessment. In order for certain responsible entities such as reliability coordinators, balancing authorities, and transmission operators to adequately perform their reliability	The SDT agrees that inter-Control Center communications play a critical role in Bulk Electric System reliability. Responsible Entities should therefore apply security measures to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring ~~and control~~ data. Since the current CIP Reliability Standards do not address this, the SDT has designed the requirement ~~requirements~~ to protect the data while it is being transmitted between inter-entity and intra-entity Control Centers.

Directives from FERC Order No. 822		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
	functions, their associated control centers must be capable of receiving and storing a variety of sensitive bulk electric system data from interconnected entities. Accordingly, we find that additional measures to protect both the integrity and availability of sensitive bulk electric system data are warranted.[60] We also understand that the attributes of the data managed by responsible entities could require different information protection controls. [61] For instance, certain types of reliability data will be sensitive to data manipulation type attacks, while other types of reliability data will be sensitive to eavesdropping type attacks aimed at collecting operational information (such as line and equipment ratings and impedances). NERC should consider the differing attributes of bulk electric system data as it assesses the development of appropriate controls. Footnotes: [59] NERC Comments at 20. [60] Protecting the integrity of bulk electric system data involves maintaining and ensuring the accuracy and consistency of inter-Control Center communications. Protecting the availability of bulk electric system data	The SDT has drafted ~~requirements~~ a requirement that allows responsible entities to apply protection to the communication links, the data, or both to satisfy the security objective consistent with the capabilities of the responsible entity's operational environment.

Directives from FERC Order No. 822		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
	involves ensuring that required data is available when needed for bulk electric system operations. [61] Moreover, in order for certain responsible entities to adequately perform their Reliability Functions, the associated control centers must be capable of receiving and storing a variety of sensitive data as specified by the IRO and TOP Standards. For instance, pursuant to Reliability Standard TOP-003-3, Requirements R1, R3 and R5, a transmission operator must maintain a documented specification for data and distribute its data specification to entities that have data required by the transmission operator's Operational Planning Analyses, Real-time Monitoring and Real-time Assessments. Entities receiving a data specification must satisfy the obligation of the documented specification.	
55	55. With regard to NERC's development of modifications responsive to our directive, we agree with NERC and other commenters that NERC should have flexibility in the manner in which it addresses the Commission's directive. Likewise, we find reasonable the principles outlined by NERC that protections for communication links and sensitive bulk electric system data communicated between bulk electric system Control Centers: (1) should not have an adverse effect on reliability, including the recognition of instances where	The SDT drafted Reliability Standard CIP-012-1 ~~requirements~~ to mitigate the risk of unauthorized disclosure or modification of Real-time Assessments and Real-time monitoring ~~and control~~ data while being transmitted between Control Centers. The SDT developed and objective-based rather than prescriptive requirement~~s~~. This approach will allow Responsible Entities flexibility in protecting these communications networks and sensitive BES data in a manner suited to each of their respective operational environments. It will also allow Responsible Entities to implement protection that considers the risks noted by the

Directives from FERC Order No. 822		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
	the introduction of latency could have negative results; (2) should account for the risk levels of assets and information being protected, and require protections that are commensurate with the risks presented; and (3) should be results-based in order to provide flexibility to account for the range of technologies and entities involved in bulk electric system communications.[62] Footnote: [62] See NERC Comments at 20-21.	Commission. The SDT identified a need to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring ~~and control~~ data regardless of asset risk level. The proposal requires protection for all Real-time Assessment and Real-time monitoring ~~and control~~ data while being transmitted between Control Centers.
56	56. We disagree with the assertion of NIPSCO and G&T Cooperatives that the risk posed by bulk electric system communication networks does not justify the costs of implementing controls. Communications between Control Centers over such networks are fundamental to the operations of the bulk electric system, and the record here does not persuade us that controls for such networks are not available at a reasonable cost (through encryption or otherwise). Nonetheless, we recognize that not all communication network components and data pose the same risk to bulk electric system reliability and may not require the same level of protection. We expect NERC to develop controls that reflect the risk posed by the asset or data being protected, and that can be implemented in	The SDT noted the FERC reference to additional Reliability Standards (TOP-003-3 and IRO-010-2) and the responsibilities to protect the data in accordance with those standards. The SDT interpreted these references as examples of potentially sensitive BES data and chose to base the CIP-012 requirements on the data specifications in TOP-003-3 and IRO-010-2~~.~~. This consolidates scoping and helps ensure that Responsible Entities mitigate the risk of the unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring ~~and control~~ data, rather than leaving the scoping of sensitive bulk electric system data to individual Responsible Entities. The SDT drafted CIP-012-1 to address confidentiality and integrity of Real-time Assessment and Real-time monitoring ~~and control~~ data. This was accomplished by drafting the

Directives from FERC Order No. 822		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
	a reasonable manner. It is important to recognize that certain entities are already required to exchange necessary real-time and operational planning data through secured networks using a "mutually agreeable security protocol," regardless of the entity's size or impact level.[63] 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. Footnote: [63] See Reliability Standards TOP-003-3, Requirement R5 and IRO-010-2, Requirement R3.	requirement to mitigate the risk from unauthorized disclosure or modification. The SDT asserts that the availability of this data is already required by the performance obligation of the TOP and IRO Reliability Standards. The SDT drafted CIP-012-1 to address the data while being transmitted. The SDT contends that this data is maintained within BES Cyber Systems, and is afforded the protections of CIP-003 through CIP-011 while at rest.
58	58. Several commenters sought clarification whether Control Centers owned by multiple registered entities would be included under the Commission's proposal. We clarify that the scope of the directed modifications apply to Control Center communications from facilities at all impact levels, regardless of ownership. The directed modification should encompass communication links and data for intra-Control Center and inter-Control Center communications.	The SDT drafted CIP-012-1 to apply to all impact levels of BES Cyber Systems (i.e., high, medium, or low impact), regardless of ownership. The SDT designed ~~requirements~~ the requirement to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring ~~and control~~ data while being transmitted between inter-entity and intra-entity BES Control Centers.

Directives from FERC Order No. 822		
Paragraph	**Directive Language**	**Consideration of Issue or Directive**
62	62. Several commenters addressed encryption and latency. Based on the record in this proceeding, it is reasonable to conclude that any lag in communication speed resulting from implementation of protections should only be measureable on the order of milliseconds and, therefore, will not adversely impact Control Center communications. Several commenters raise possible technical implementation difficulties with integrating encryption technologies into their current communications networks. Such technical issues should be considered by the standard drafting team when developing modifications in response to this directive, and may be resolved, e.g., by making certain aspects of the revised CIP Standards eligible for Technical Feasibility Exceptions.	The SDT developed an objective-based rather than prescriptive requirement~~s~~. This approach will allow Responsible Entities flexibility in mitigating the risk of unauthorized disclosure or modification of Real-time Assessments and Real-time monitoring data in a manner suited to each of their respective operational environments. It will also allow Responsible Entities to implement protection that considers the risks noted by the Commission.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Violation Risk Factor and Violation Severity Level Justifications

Project 2016-02 Modifications to CIP Standards

This document provides the standard drafting team's (SDT's) justification for assignment of violation risk factors (VRFs) and violation severity levels (VSLs) for each requirement in **CIP-012-1**. Each requirement is assigned a VRF and a VSL. These elements support the determination of an initial value range for the Base Penalty Amount regarding violations of requirements in FERC-approved Reliability Standards, as defined in the Electric Reliability Organizations (ERO) Sanction Guidelines. The SDT applied the following NERC criteria and FERC Guidelines when developing the VRFs and VSLs for the requirements.

NERC Criteria for Violation Risk Factors

High Risk Requirement

A requirement that, if violated, could directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures, or could hinder restoration to a normal condition.

Medium Risk Requirement

A requirement that, if violated, could directly affect the electrical state or the capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System. However, violation of a medium risk requirement is unlikely to lead to Bulk Electric System instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System. However, violation of a medium risk requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to Bulk Electric System instability, separation, or cascading failures, nor to hinder restoration to a normal condition.

Lower Risk Requirement

A requirement that is administrative in nature and a requirement that, if violated, would not be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System; or, a requirement that is administrative in nature and a requirement in a planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.

FERC Guidelines for Violation Risk Factors

Guideline (1) – Consistency with the Conclusions of the Final Blackout Report

FERC seeks to ensure that VRFs assigned to Requirements of Reliability Standards in these identified areas appropriately reflect their historical critical impact on the reliability of the Bulk-Power System. In the VSL Order, FERC listed critical areas (from the Final Blackout Report) where violations could severely affect the reliability of the Bulk-Power System:

- Emergency operations
- Vegetation management
- Operator personnel training
- Protection systems and their coordination
- Operating tools and backup facilities
- Reactive power and voltage control
- System modeling and data exchange
- Communication protocol and facilities
- Requirements to determine equipment ratings
- Synchronized data recorders
- Clearer criteria for operationally critical facilities
- Appropriate use of transmission loading relief.

Guideline (2) – Consistency within a Reliability Standard

FERC expects a rational connection between the sub-Requirement VRF assignments and the main Requirement VRF assignment.

Guideline (3) – Consistency among Reliability Standards

FERC expects the assignment of VRFs corresponding to Requirements that address similar reliability goals in different Reliability Standards would be treated comparably.

Guideline (4) – Consistency with NERC's Definition of the Violation Risk Factor Level

Guideline (4) was developed to evaluate whether the assignment of a particular VRF level conforms to NERC's definition of that risk level.

Guideline (5) – Treatment of Requirements that Co-mingle More Than One Obligation

Where a single Requirement co-mingles a higher risk reliability objective and a lesser risk reliability objective, the VRF assignment for such Requirements must not be watered down to reflect the lower risk level associated with the less important objective of the Reliability Standard.

NERC Criteria for Violation Severity Levels

VSLs define the degree to which compliance with a requirement was not achieved. Each requirement must have at least one VSL. While it is preferable to have four VSLs for each requirement, some requirements do not have multiple "degrees" of noncompliant performance and may have only one, two, or three VSLs.

VSLs should be based on NERC's overarching criteria shown in the table below:

Lower VSL	Moderate VSL	High VSL	Severe VSL
The performance or product measured almost meets the full intent of the requirement.	The performance or product measured meets the majority of the intent of the requirement.	The performance or product measured does not meet the majority of the intent of the requirement, but does meet some of the intent.	The performance or product measured does not substantively meet the intent of the requirement.

FERC Order of Violation Severity Levels

The FERC VSL guidelines are presented below, followed by an analysis of whether the VSLs proposed for each requirement in the standard meet the FERC Guidelines for assessing VSLs:

Guideline (1) – Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance

Compare the VSLs to any prior levels of non-compliance and avoid significant changes that may encourage a lower level of compliance than was required when levels of non-compliance were used.

Guideline (2) – Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties

A violation of a "binary" type requirement must be a "Severe" VSL.

Do not use ambiguous terms such as "minor" and "significant" to describe noncompliant performance.

Guideline (3) – Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement

VSLs should not expand on what is required in the requirement.

Guideline (4) – Violation Severity Level Assignment Should Be Based on a Single Violation, Not on a Cumulative Number of Violations

Unless otherwise stated in the requirement, each instance of non-compliance with a requirement is a separate violation. Section 4 of the Sanction Guidelines states that assessing penalties on a per violation per day basis is the "default" for penalty calculations.

VRF Justifications for CIP-012-1, Requirement R1	
Proposed VRF	**Medium**
NERC VRF Discussion	A VRF of Medium was assigned to this requirement. Cyber security plans enable effective implementation of the CIP standard's requirements to mitigate the risk of the unauthorized disclosure or modification of data used for Real-time Assessments and Real-time monitoring while being transmitted between Control Centers.
FERC VRF G1 Discussion Guideline 1- Consistency with Blackout Report	N/A
FERC VRF G2 Discussion Guideline 2- Consistency within a Reliability Standard	N/A
FERC VRF G3 Discussion Guideline 3- Consistency among Reliability Standards	The requirement complements CIP-005-1, Requirement R1, CIP-006-6, Requirement R1, and CIP-007-6, Requirement R1 which are related to security of networks and communications components. The proposed VRF is consistent with these related requirements.
FERC VRF G4 Discussion Guideline 4- Consistency with NERC Definitions of VRFs	Failure to have a cyber security plan would not, under Emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.
FERC VRF G5 Discussion	N/A

VRF Justifications for CIP-012-1, Requirement R1	
Proposed VRF	**Medium**
Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation	

VSLs for CIP-012-1, Requirement R1			
Lower	**Moderate**	**High**	**Severe**
N/A	The Responsible Entity documented its plan(s) but failed to include one of the applicable parts of the plan as specified in Requirement R1.	The Responsible Entity documented its plan(s) but failed to include two of the applicable parts of the plan as specified in Requirement R1.	The Responsible Entity failed to document plan(s) for Requirement R1; Or The Responsible Entity failed to implement any Part of its plan(s) for Requirement R1, except under CIP Exceptional Circumstances.

VSL Justifications for CIP-012-1 Requirements R1	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The requirement is new. Therefore, the proposed VSL does not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The requirement is for the Responsible Entity to implement one or more documented plan(s) as specified in Requirement R1. The moderate VSL addresses where the Responsible Entity documented its plan(s) but failed to include one of the applicable parts of the plan as specified in Requirement R1. The high VSL addresses where the Responsible Entity documented its plan(s) but failed to include two of the applicable parts of the plan as specified in Requirement R1. The severe VSL addresses where the Responsible Entity failed to document plan(s) for Requirement R1, or where the Responsible Entity failed to implement plan(s) for Requirement R1.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL uses the same terminology as used in the associated requirement and is, therefore, consistent with the requirement.

FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Each VSL is based on a single violation and not cumulative violations.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Violation Risk Factor and Violation Severity Level Justifications

Project 2016-02 Modifications to CIP Standards

This document provides the standard drafting team's (SDT's) justification for assignment of violation risk factors (VRFs) and violation severity levels (VSLs) for each requirement in **CIP-012-1**. Each requirement is assigned a VRF and a VSL. These elements support the determination of an initial value range for the Base Penalty Amount regarding violations of requirements in FERC-approved Reliability Standards, as defined in the Electric Reliability Organizations (ERO) Sanction Guidelines. The SDT applied the following NERC criteria and FERC Guidelines when developing the VRFs and VSLs for the requirements.

NERC Criteria for Violation Risk Factors

High Risk Requirement

A requirement that, if violated, could directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures, or could hinder restoration to a normal condition.

Medium Risk Requirement

A requirement that, if violated, could directly affect the electrical state or the capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System. However, violation of a medium risk requirement is unlikely to lead to Bulk Electric System instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System. However, violation of a medium risk requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to Bulk Electric System instability, separation, or cascading failures, nor to hinder restoration to a normal condition.

Lower Risk Requirement
A requirement that is administrative in nature and a requirement that, if violated, would not be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System; or, a requirement that is administrative in nature and a requirement in a planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.

FERC Guidelines for Violation Risk Factors

Guideline (1) – Consistency with the Conclusions of the Final Blackout Report

FERC seeks to ensure that VRFs assigned to Requirements of Reliability Standards in these identified areas appropriately reflect their historical critical impact on the reliability of the Bulk-Power System. In the VSL Order, FERC listed critical areas (from the Final Blackout Report) where violations could severely affect the reliability of the Bulk-Power System:

- Emergency operations
- Vegetation management
- Operator personnel training
- Protection systems and their coordination
- Operating tools and backup facilities
- Reactive power and voltage control
- System modeling and data exchange
- Communication protocol and facilities
- Requirements to determine equipment ratings
- Synchronized data recorders
- Clearer criteria for operationally critical facilities
- Appropriate use of transmission loading relief.

Guideline (2) – Consistency within a Reliability Standard

FERC expects a rational connection between the sub-Requirement VRF assignments and the main Requirement VRF assignment.

Guideline (3) – Consistency among Reliability Standards

FERC expects the assignment of VRFs corresponding to Requirements that address similar reliability goals in different Reliability Standards would be treated comparably.

Guideline (4) – Consistency with NERC's Definition of the Violation Risk Factor Level

Guideline (4) was developed to evaluate whether the assignment of a particular VRF level conforms to NERC's definition of that risk level.

Guideline (5) – Treatment of Requirements that Co-mingle More Than One Obligation

Where a single Requirement co-mingles a higher risk reliability objective and a lesser risk reliability objective, the VRF assignment for such Requirements must not be watered down to reflect the lower risk level associated with the less important objective of the Reliability Standard.

NERC Criteria for Violation Severity Levels

VSLs define the degree to which compliance with a requirement was not achieved. Each requirement must have at least one VSL. While it is preferable to have four VSLs for each requirement, some requirements do not have multiple "degrees" of noncompliant performance and may have only one, two, or three VSLs.

VSLs should be based on NERC's overarching criteria shown in the table below:

Lower VSL	Moderate VSL	High VSL	Severe VSL
The performance or product measured almost meets the full intent of the requirement.	The performance or product measured meets the majority of the intent of the requirement.	The performance or product measured does not meet the majority of the intent of the requirement, but does meet some of the intent.	The performance or product measured does not substantively meet the intent of the requirement.

FERC Order of Violation Severity Levels

The FERC VSL guidelines are presented below, followed by an analysis of whether the VSLs proposed for each requirement in the standard meet the FERC Guidelines for assessing VSLs:

Guideline (1) – Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance

Compare the VSLs to any prior levels of non-compliance and avoid significant changes that may encourage a lower level of compliance than was required when levels of non-compliance were used.

Guideline (2) – Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties

A violation of a "binary" type requirement must be a "Severe" VSL.

Do not use ambiguous terms such as "minor" and "significant" to describe noncompliant performance.

Guideline (3) – Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement

VSLs should not expand on what is required in the requirement.

Guideline (4) – Violation Severity Level Assignment Should Be Based on a Single Violation, Not on a Cumulative Number of Violations

Unless otherwise stated in the requirement, each instance of non-compliance with a requirement is a separate violation. Section 4 of the Sanction Guidelines states that assessing penalties on a per violation per day basis is the "default" for penalty calculations.

VRF Justifications for CIP-012-1, Requirement R1	
Proposed VRF	**Medium**
NERC VRF Discussion	A VRF of Medium was assigned to this requirement. Cyber security plans enable effective implementation of the CIP standard's requirements to mitigate the risk of the unauthorized disclosure or modification of data used for Real-time Assessments and Real-time monitoring while being transmitted between Control Centers.
FERC VRF G1 Discussion Guideline 1- Consistency with Blackout Report	N/A
FERC VRF G2 Discussion Guideline 2- Consistency within a Reliability Standard	N/A
FERC VRF G3 Discussion Guideline 3- Consistency among Reliability Standards	The requirement complements CIP-005-1, Requirement R1, CIP-006-6, Requirement R1, and CIP-007-6, Requirement R1 which are related to security of networks and communications components. The proposed VRF is consistent with these related requirements.
FERC VRF G4 Discussion Guideline 4- Consistency with NERC Definitions of VRFs	Failure to have a cyber security plan would not, under Emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.
FERC VRF G5 Discussion	N/A

VRF Justifications for CIP-012-1, Requirement R1	
Proposed VRF	**Medium**
Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation	

VSLs for CIP-012-1, Requirement R1			
Lower	**Moderate**	**High**	**Severe**
N/A	The Responsible Entity documented its plan(s) but failed to include one of the applicable parts of the plan as specified in Requirement R1.	The Responsible Entity documented its plan(s) but failed to include two of the applicable parts of the plan as specified in Requirement R1.	The Responsible Entity failed to document plan(s) for Requirement R1; Or The Responsible Entity failed to implement any Part of its plan(s) for Requirement R1, except under CIP Exceptional Circumstances.

VSL Justifications for CIP-012-1 Requirements R1	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The requirement is new. Therefore, the proposed VSL does not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The requirement is for the Responsible Entity to implement one or more documented plan(s) as specified in Requirement R1. The moderate VSL addresses where the Responsible Entity documented its plan(s) but failed to include one of the applicable parts of the plan as specified in Requirement R1. The high VSL addresses where the Responsible Entity documented its plan(s) but failed to include two of the applicable parts of the plan as specified in Requirement R1. The severe VSL addresses where the Responsible Entity failed to document plan(s) for Requirement R1, or where the Responsible Entity failed to implement plan(s) for Requirement R1.~~.~~
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL uses the same terminology as used in the associated requirement and is, therefore, consistent with the requirement.

FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Each VSL is based on a single violation and not cumulative violations.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

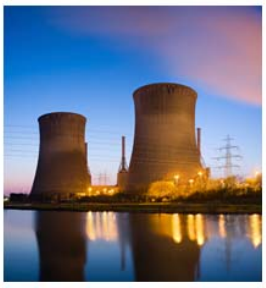
DRAFT

Cyber Security – Communications Between Control Centers

Implementation Guidance for CIP-012-1

March 2018

RELIABILITY | ACCOUNTABILITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Introduction

The Project 2016-02 SDT drafted this Implementation Guidance to provide example approaches for compliance with CIP-012-1. Implementation Guidance does not prescribe the only approach, but highlights one or more approaches that would be effective in achieving compliance with the standard. Because Implementation Guidance only provides examples, entities may choose alternative approaches that better fit their individual situations[1].

Responsible Entities may find it useful to consider this Implementation Guidance document along with the additional context and background provided in the SDT-developed Technical Rationale and Justification for CIP-012-1 document.

Background

The Commission issued Order No. 822 on January 21, 2016. Order 822 approving seven CIP Reliability Standards and new or modified definitions, and directed modifications be made to the CIP Reliability Standards. Among other items, the Commission directed NERC to "develop modifications to the CIP Reliability Standards to require responsible entities to implement controls to protect, at a minimum, communication links and sensitive bulk electric system data communicated between bulk electric system Control Centers in a manner that is appropriately tailored to address the risks posed to the bulk electric system by the assets being protected (i.e., high, medium, or low impact)." (Order 822, Paragraph 53)

In response to the directive in Order No. 822, the Project 2016-02 standard drafting team (SDT) drafted Reliability Standard CIP-012-1 to require Responsible Entities to implement controls to protect sensitive Bulk Electric System (BES) data and communications links between BES Control Centers. Due to the sensitivity of the data being communicated between Control Centers, the standard applies to all impact levels (i.e., high, medium, or low impact).

The SDT drafted requirements to provide Responsible Entities the latitude to protect the communication links, the data, or both, to satisfy the security objective consistent with the capabilities of the Responsible Entity's operational environment.

[1] NERC's Compliance Guidance Policy

Requirements

R1. *The Responsible Entity shall implement one or more documented plan(s) to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring data while being transmitted between any Control Centers. This requirement excludes oral communications. The plan shall include: [Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. Identification of security protection used to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers;

1.2. Identification of where the Responsible Entity applied security protection for transmitting Real-time Assessment and Real-time monitoring and control data between Control Centers; and

1.3. If the Control Centers are owned or operated by different Responsible Entities, identify the responsibilities of each Responsible Entity for applying security protection to the transmission of Real-time Assessment and Real-time monitoring data between those Control Centers.

General Considerations

Plan Development

As noted in the Technical Rationale and Justification for CIP-012-1, the focus of Requirement R1 is implementing a documented plan to protect information that is critical to the real-time operations of the Bulk Electric System while in transit between applicable Control Centers. The number of plan(s) and their content may vary depending on a Responsible Entity's management structure and operating conditions. The Responsible Entity may document as many plans as necessary to meet its needs. For instance, a Responsible Entity may choose to document one plan per Control Center or choose an all-inclusive, single plan for its Control Center communication environment. A Responsible Entity may choose to document one plan for communications between Control Centers it owns and a separate plan for communications between its Control Centers and the Control Centers of a neighboring Entity. The number and structure of the plans is at the discretion of the Responsible Entity as long as the plan(s) include the required elements described in parts 1.1, 1.2, and 1.3 of Requirement R1.

Identification of Security Protection

Entities have latitude to identify and choose which security protection is used to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers.

This security protection could consist of logical protection, physical protection, or some combination of both. To determine security protection, the requirement specifies that it must mitigate the risk of unauthorized disclosure or modification of applicable data.

Security protection implementation can be demonstrated in many ways. If a Responsible Entity uses physical protection, it may demonstrate implementation through review of an applicable Control Center floor plan with details subsequently confirmed through visual inspection, which identifies the physical security measures in place protecting the communication link. If the Responsible Entity uses logical protection, it may demonstrate implementation through an export of the device configuration which applies the security protection. Alternatively, a Responsible Entity may demonstrate implementation through security control monitoring, using an automated monitoring tool to generate reports on the encryption service used to protect a communications link.

Identification of Where Security Protection is Applied by the Responsible Entity

A Responsible Entity should consider its environment when identifying where security protections should be applied. One approach is to implement security within the Control Center itself to ensure that data confidentiality and integrity is protected throughout the transmission. The Responsible Entity can identify where security protection is applied using a logical or physical location The application of security in accordance with CIP-012 requirements does not add additional assets to the scope of the CIP Reliability Standards. Locations of applied security protection may vary based on many factors such as impact levels of the Control Center, different technologies, or infrastructures.

Identification of where a Responsible Entity applies security protection could be demonstrated with a list or a Control Center diagram showing either physical or logical security controls. Physical diagrams may require visual confirmation of these controls. These diagrams or a list could be included within the plan developed for R1. A Responsible Entity could also use labels to identify on-site devices where CIP-012 security protection is applied.

When exchanging data between two entities, if a Responsible Entity only manages one end of a communication link, the Responsible Entity is not responsible for identifying where the security protection is applied by the neighboring entity with whom it is exchanging data. However, if a Responsible Entity has taken responsibility for

both ends of the communication link (such as by placing a router within the neighboring entity's data center), then the Responsible Entity shall identify where the security protection is applied at both ends of the link. Similarly, if a Responsible Entity owns and operates both Control Centers which are exchanging data (such as in the case of a primary and backup Control Center), then the Responsible Entity shall identify where security protection is applied at both ends of the link.

Identification of Responsibilities when the Control Centers are Owned or Operated by Different Responsible Entities

The Technical Rationale and Justification for CIP-012-1 identifies key considerations in the Control Center Ownership section when communications between Control Centers with different owners or operators. Many operational relationships between Responsible Entities are unique. Consequently, there is no single way to identify responsibilities for applying security protection to the transmission of Real-time Assessment and Real-time monitoring data between Control Centers.

Implementation of responsibilities could also be demonstrated in many ways. Some examples include a joint procedure, a memorandum of understanding, or meeting minutes between the two parties where responsibilities are defined.

Reference Model

For this Implementation Guidance, the SDT uses a basic reference model of Primary and Backup Control Centers (Entity Alpha) to illustrate approaches to demonstrating compliance. These Control Centers communicate to each other and to a neighboring entity's Control Center (Entity Beta) in configurations outlined by the diagrams in this section. The SDT recognizes that the reference model does not contain many of the complexities of a real Control Center. For this Implementation Guidance, the registration or functions performed in the reference model Control Center are also not considered. A high level block diagram of the basic reference model is shown below in Figure 1. This Implementation Guidance is developed from the perspective of Entity Alpha.

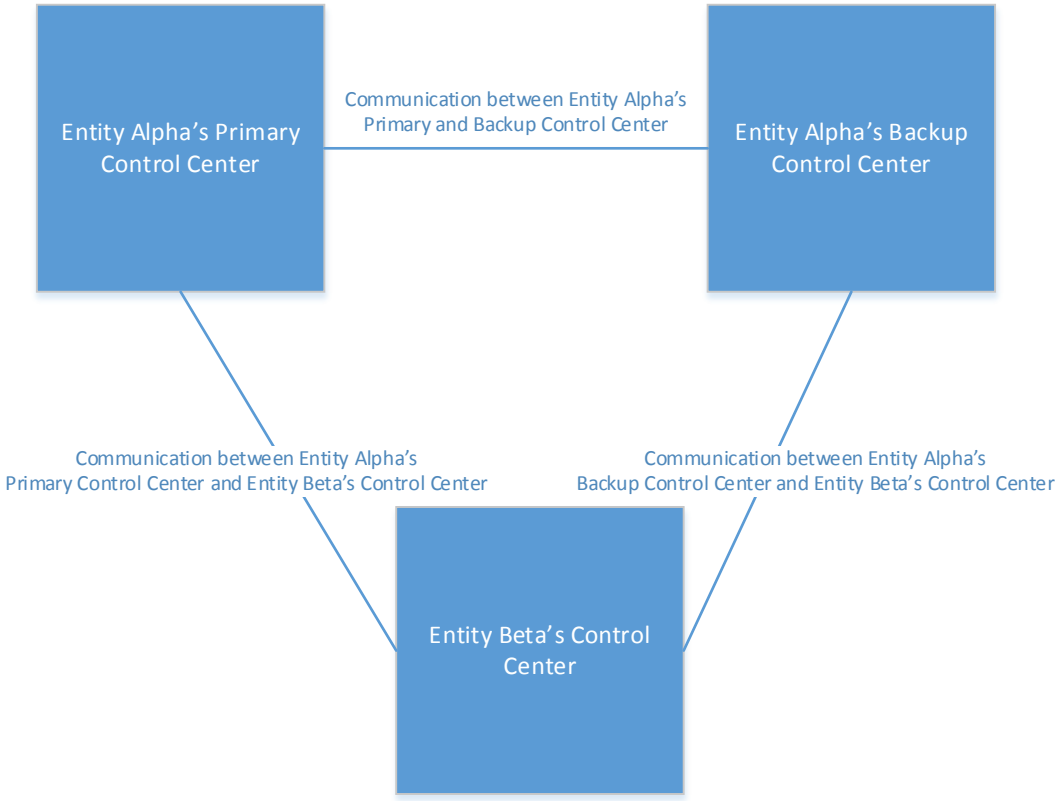


Figure 1: High Level Block Diagram of Reference Model Control Centers

Reference Model Discussion

Requirement R1 requires the implementation of a documented plan. To comply with requirement R1, one approach to a plan is to first determine which communications are in scope of CIP-012-1. There are multiple ways to identify an entity's scope in R1. For example, Entity Alpha in the reference model may first identify the Control Centers with which it communicates. Entity Alpha would determine that there are three: Entity Alpha's Primary Control Center, Entity Alpha's Backup Control Center, and Entity Beta's Control Center. Entity Alpha does not need to consider whether Entity Beta further shares its data with another Entity. That is the responsibility of Entity Beta and is outside of Entity Alpha's purview. Additionally, Entity Alpha does not need to consider any communications to other non-Control Center facilities such as generating plants or substations. These communications are out of scope for CIP-012-1.

Now that Entity Alpha has identified the Control Centers with which it communicates, Entity Alpha identifies either: (1) the Real-time Assessment and Real-time monitoring data; or (2) communication links which are used to transmit Real-time Assessment and Real-time monitoring data between Control Centers. In either case, Entity Alpha should refer to the data specification for Real-time Assessment and Real-time monitoring data identified

in TOP-003-3 and IRO-010-2. For this reference model scenario, identifying the communication links used to transmit Real-time Assessment and Real-time monitoring data may be the most straightforward approach. Through an evaluation of communication links between Control Centers and an evaluation of how it transmits and receives Real-time Assessment and Real-time monitoring data, Entity Alpha determined that it communicates applicable data between its primary and backup Control Centers across a single communication link. Entity Alpha also determined that it communicates applicable data to and from Entity Beta's Control Center across one of two links that originate from either Entity Alpha's primary or backup Control Center using the Inter-Control Center Communications Protocol (ICCP).

With an identified scope of communications links, Entity Alpha now considers the three required elements of its required communications between Control Centers for its plan.

Identification of Security Protection

- Entity Alpha must ensure that protection is applied where identified in its CIP-012-1 plan. The protection must also meet the security objective of mitigating the risk of unauthorized disclosure or modification of applicable data while in transit between Control Centers. The identification of security protection could be demonstrated by a network diagram similar to that shown in Figure 2 or Figure 3.
- In a simple case where the security protection is applied sufficiently close to the Control Center, such as within the Physical Security Perimeter of the Control Center, Entity Alpha may use a single security protection method to meet the security objective. For this case, shown in Figure 2, Entity Alpha implements a Virtual Private Network (VPN) connection across a private leased communication circuit for each of its three in-scope communication links. To meet the security objective, Entity Alpha further states that its VPN uses Internet Protocol security (IPsec) with encryption.
- For more complex scenarios, Entity Alpha may need to use a combination of security controls. For instance, in Figure 3, Entity Alpha uses a combination of physical security controls (physical access control) and logical security controls (encrypted communications consistent with the first scenario above) to meet the security objective.
- While these scenarios are all specific to communication links, it is possible that Entity Alpha and Entity Beta achieve the security objective by applying protection to the data rather than the communication links. In this scenario, the application enabling the data exchange between Control Centers may be capable of applying security controls directly to the data. These security controls mitigate the risk of unauthorized disclosure or modification of applicable data rather than relying on lower level network services to provide this security. For instance, Entity Alpha and Entity Beta may apply security protection at the application layer by using Secure ICCP to exchange applicable data. According to a report released by Sandia National Labs[2], Secure ICCP provides "data integrity indirectly by providing a cryptographic checksum. Secure ICCP provides data confidentiality by encrypting ICCP data exchanges." Methods other than Secure ICCP could also be used to apply security protection to the data at the application layer.
- It is theoretically possible that Entity Alpha and Entity Beta could exchange Real-time Assessment data between Control Centers by email. In that scenario, one approach may be for Entity Alpha to email the applicable data to Entity Beta's Control Center in a protected container such as an encrypted zip file. Entity Alpha and Entity Beta can then exchange the password to that encrypted container through another method, such as by phone. While the notional example of protecting data exchanged by email is a useful illustration of how to achieve the security objective of CIP-012-1, it is extremely unlikely to be used in practice. The characteristics of email communication are inconsistent with the requirements of Real-time data exchange.

[2] https://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/19-Secure_ICCP_Integration.pdf

Identification of Where Security Protection is Applied by the Responsible Entity

Similar to the identification of security protection above, the identification of where security protection is applied can also be demonstrated by a network diagram similar to those found in Figures 2 and 3.

- Figure 2 shows the identification where CIP-012-1 security protection is applied for the Entity Alpha reference model when a single encrypted tunnel is used to implement the required protection. Entity Alpha has identified that security protection is applied at each of its Control Centers on the external Ethernet interface on the WAN router. While the diagram depicts where Entity Beta has applied security protection for illustrative purposes, Entity Alpha is not responsible for identifying where Entity Beta has applied security protection.
- In order to understand the application of security protection in context of who controls the communication link, it may be helpful to identify both where CIP-012-1 security protection is applied and the location of the telecommunications carrier (telco) demarcation point. Figure 3 provides such an example where the telco demarcation point may not be within the Control Center and based the facts and circumstances surrounding this scenario, Entity Alpha has implemented a combination of security controls to comply with CIP-012-1. In this scenario, Entity Alpha identifies that it has applied physical security protection for its PSP and continuing for its WAN router and that it has applied logical security protection (encryption) at the WAN router. Entity Alpha has also identified the telco demarcation point at a point in the telecommunications cabling connecting to Entity Alpha's WAN router, perhaps at a punch down block for example. In Figure 3, the telco demarcation point is inside the same room as the WAN router. The telco demarcation points are referenced in the drawing for clarity, but are not part of the plan.
- The data-centric scenario described above is less intuitive for identifying where security protection is applied by Entity Alpha. If security protection is applied at the application layer (such as Secure ICCP), Entity Alpha could reasonably identify the application or service applying the security (such as the Secure ICCP service) as the location of where security protection is applied.

Identification of Responsibilities when the Control Centers are Owned or Operated by Different Responsible Entities

Entity Alpha and Entity Beta may determine they each are responsible for one end of the VPN configuration on their respective WAN routers. Entity Alpha and Entity Beta have agreed to a 30 character pre-shared key for IPSec authentication.

Rather than use a pre-shared key, Entity Alpha and Entity Beta may decide to use digital certificates for the IPSec authentication using a trusted certificate authority. In that scenario, Entity Alpha and Entity Beta would agree on who is the party responsible for managing the certificate authority.

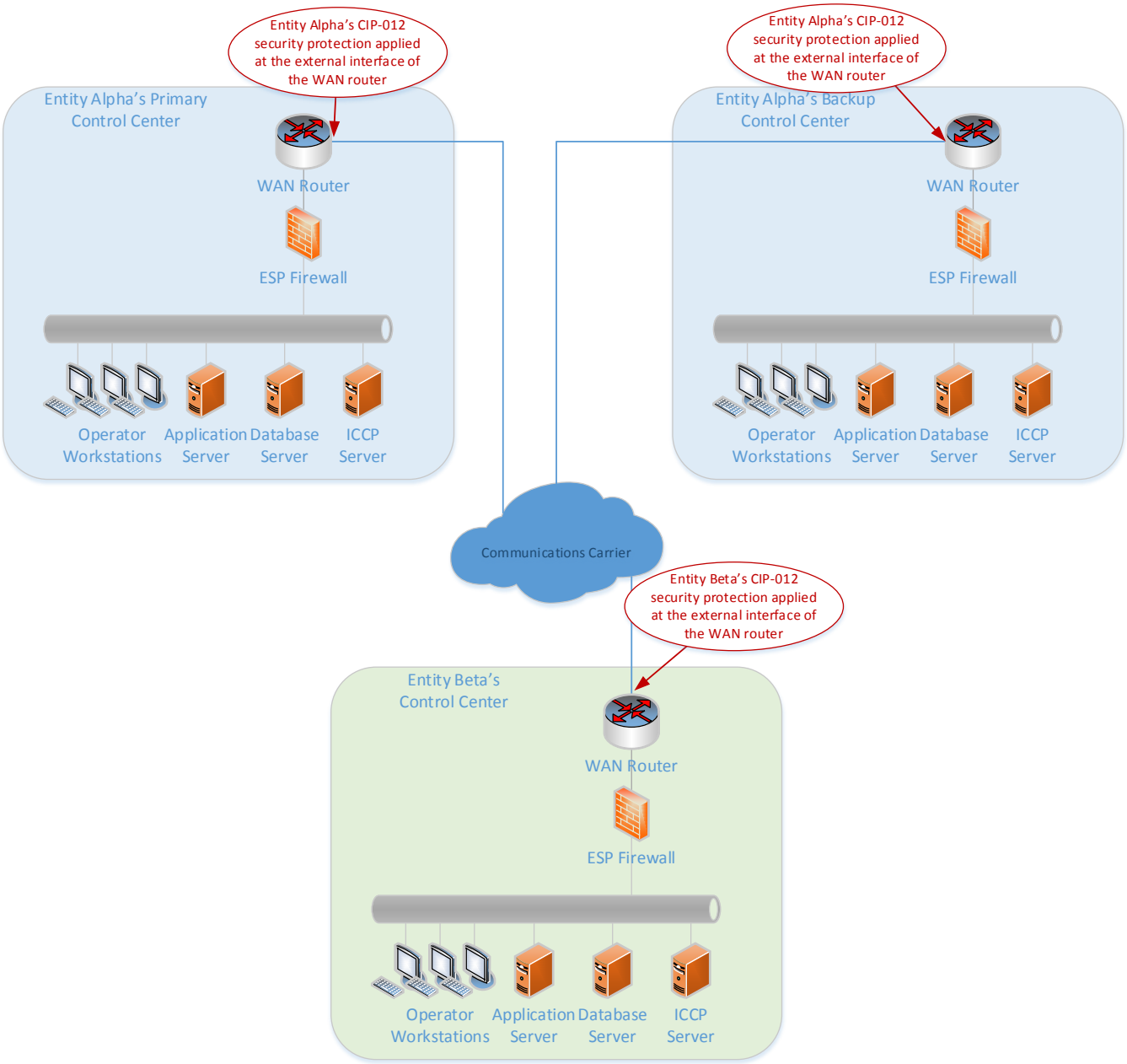


Figure 2: Network diagram and identification of where security protection is applied

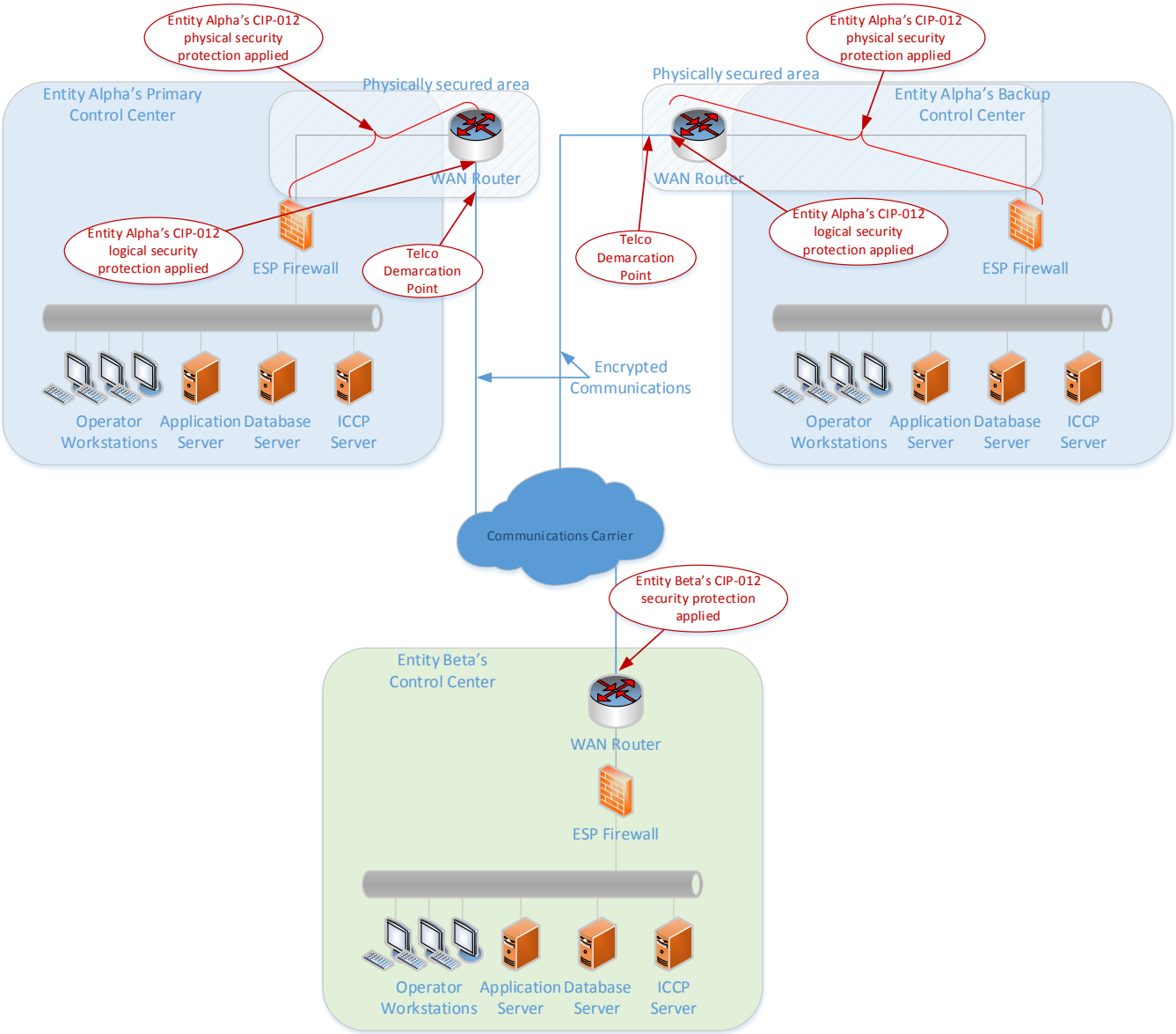


Figure 3: Network diagram using a combination of controls for CIP-012-1

References

Mitre Common Weakness Enumeration (CWE™) list of software weakness types
https://cwe.mitre.org/data/definitions/327.html

Cryptographic Standards and Guidelines
https://csrc.nist.gov/Projects/Cryptographic-Standards-and-Guidelines

NIST Special Publication 800-175B
Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-175B.pdf

Guide to Cryptography
https://www.owasp.org/index.php/Guide_to_Cryptography#Symmetric_Cryptography

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

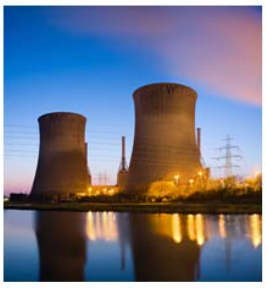
DRAFT

Cyber Security – Communications Between Control Centers

Implementation Guidance for CIP-012-1

~~November~~March~~,~~ 2018~~7~~

RELIABILITY | ACCOUNTABILITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Introduction

~~The Commission issued Order No. 822 on January 21, 2016. Order 822 approved seven CIP Reliability Standards and new or modified definitions, and directed modifications be made to the CIP Reliability Standards. Among other items, the Commission directed NERC to "develop modifications to the CIP Reliability Standards to require responsible entities to implement controls to protect, at a minimum, communication links and sensitive bulk electric system data communicated between bulk electric system Control Centers in a manner that is appropriately tailored to address the risks posed to the bulk electric system by the assets being protected (i.e., high, medium, or low impact)." (Order 822, Paragraph 53)~~

~~In response to the directive in Order No. 822, the Project 2016-02 standard drafting team (SDT) drafted Reliability Standard CIP-012-1 to require Responsible Entities to implement controls to protect sensitive Bulk Electric System (BES) data and communications links between BES Control Centers. Due to the sensitivity of the data being communicated between Control Centers, the standard applies to all impact levels (i.e., high, medium, or low impact).~~

~~The SDT drafted requirements to provide Responsible Entities the latitude to protect the communication links, the data, or both, to satisfy the security objective consistent with the capabilities of the Responsible Entity's operational environment. Requirement R1 requires Responsible Entities to document one or more plans that protect Real-time Assessment and Real-time monitoring and control data while being transmitted between Control Centers. The plan(s) must address how the Responsible Entity will mitigate the risk of unauthorized disclosure or modification of the applicable data. Requirement R2 covers implementation of the plan developed according to Requirement R1.~~

The Project 2016-02 SDT drafted this Implementation Guidance to provide example approaches for compliance with CIP-012-1. Implementation Guidance does not prescribe the only approach, but highlights one or more approaches that would be effective in achieving compliance with the standard. Because Implementation Guidance only provides examples, entities may choose alternative approaches that better fit their individual situations[1].

Responsible Entities may find it useful to consider this Implementation Guidance document along with the additional context and background provided in the SDT-developed Technical Rationale and Justification for CIP-012-1 document.

Background

The Commission issued Order No. 822 on January 21, 2016. Order 822 approving ~~approved~~ seven CIP Reliability Standards and new or modified definitions, and directed modifications be made to the CIP Reliability Standards. Among other items, the Commission directed NERC to "develop modifications to the CIP Reliability Standards to require responsible entities to implement controls to protect, at a minimum, communication links and sensitive bulk electric system data communicated between bulk electric system Control Centers in a manner that is appropriately tailored to address the risks posed to the bulk electric system by the assets being protected (i.e., high, medium, or low impact)." (Order 822, Paragraph 53)

In response to the directive in Order No. 822, the Project 2016-02 standard drafting team (SDT) drafted Reliability Standard CIP-012-1 to require Responsible Entities to implement controls to protect sensitive Bulk Electric System (BES) data and communications links between BES Control Centers. Due to the sensitivity of the data being communicated between Control Centers, the standard applies to all impact levels (i.e., high, medium, or low impact).

The SDT drafted requirements to provide Responsible Entities the latitude to protect the communication links, the data, or both, to satisfy the security objective consistent with the capabilities of the Responsible Entity's operational environment.

[1] NERC's Compliance Guidance Policy

Requirements

R1. *The Responsible Entity shall ~~develop~~ implement one or more documented plan(s) to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring ~~and control~~ data while being transmitted between any Control Centers. This requirement excludes oral communications. The plan shall include: [Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. Identification of security protection used to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring ~~and control~~ data while being transmitted between Control Centers;

1.2. Identification of where the Responsible Entity applied ~~demarcation point(s) where~~ security protection ~~is applied~~ for transmitting Real-time Assessment and Real-time monitoring and control data between Control Centers; and

1.3. If the Control Centers are owned or operated ~~Identification of roles and responsibilities of each Responsible Entity for applying security protection to the transmission of Real-time Assessment and Real-time monitoring and control data between Control Centers, when the Control Centers are owned or operated~~ by different Responsible Entities, identify the responsibilities of each Responsible Entity for applying security protection to the transmission of Real-time Assessment and Real-time monitoring data between those Control Centers.

~~**R2.** *The Responsible Entity shall implement the plan(s) specified in Requirement R1, except under CIP Exceptional Circumstances.*~~

General Considerations

Plan Development

~~General Considerations for R1~~

As noted in the Technical Rationale and Justification for CIP-012-1, the focus of Requirement R1 is ~~on developing~~ implementing ~~a~~ a documented plan to protect information that is critical to the real-time operations of the Bulk Electric System while in transit between applicable Control Centers. The number of plan(s) and their content may vary depending on a Responsible Entity's management structure and operating conditions. The Responsible Entity may document as many plans as necessary to meet its needs. For instance, a Responsible Entity may choose to document one plan per Control Center or ~~it may~~ choose an all-inclusive, single plan for its Control Center communication environment. ~~to document everything in a single plan.~~ A Responsible Entity may choose to document one plan for communications between Control Centers it owns and a separate plan for communications between its Control Centers and the Control Centers of a neighboring Entity. The number and structure of the plans is at the discretion of the Responsible Entity as long as the plan(s) include the required elements described in parts 1.1, 1.2, and 1.3 of Requirement R1.

Identification of Security Protection

Entities have latitude to identify and choose ~~determine~~ which security protection~~s~~ ~~are~~ is used to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring ~~and control~~ data while being transmitted between Control Centers ~~and should identify those protections accordingly~~.

This security protection could consist of logical protection, physical protection, or some combination of both. To determine security protection, the requirement specifies that it must mitigate the risk of unauthorized disclosure or modification of applicable data.

Security protection implementation can be demonstrated in many ways. If a Responsible Entity uses physical protection, it may demonstrate implementation through review of an applicable Control Center floor plan~~,~~ with details subsequently confirmed through visual inspection, which identifies the physical security measures in place protecting the communication link. If the Responsible Entity uses logical protection, it may demonstrate implementation through an export of the device configuration which applies the security protection. Alternatively, a Responsible Entity may demonstrate implementation through security control monitoring, using an automated monitoring tool to generate reports on the encryption service used to protect a communications link.

Identification of ~~Demarcation Point(s)~~ Where Security Protection is Applied by the Responsible Entity

A Responsible Entity should consider its environment ~~to determine an effective solution~~ when identifying ~~the demarcation points~~ where security protections ~~are~~ should be applied. One approach ~~to identifying a demarcation point~~ is to implement security ~~place the demarcation point~~ within the Control Center ~~so the confidentiality and integrity of the data is protected throughout the transmission~~itself to ensure that data confidentiality and integrity is protected throughout the transmission. The Responsible Entity can ~~choose either a physical or logical demarcation point~~ identify where security protection is applied using a logical or physical location~~. Demarcation points identified by the Responsible Entity do not add additional assets to the scope of the CIP Reliability Standards. The demarcation point identification ensures that each Responsible Entity identifies clear demarcation of where the protection is applied to the in-scope data. Demarcation points~~ The application of security in accordance with CIP-012 requirements does not add additional assets to the scope of the CIP Reliability Standards. Locations of applied security protection may vary based on many factors such as impact levels of the Control Center, different technologies, or infrastructures.

Identification of where a Responsible Entity applies security protection could be demonstrated with a list or a Control Center diagram showing either physical or logical security controls. Physical diagrams may require visual confirmation of these controls. These diagrams or a list could be included within the plan developed for R1. A Responsible Entity could also use labels to identify on-site devices where CIP-012 security protection is applied.

When exchanging data between two entities, if a Responsible Entity only manages one end of a communication link, the Responsible Entity is not responsible for identifying where the security protection is applied by the neighboring entity with whom it is exchanging data. However, if a Responsible Entity has taken responsibility for both ends of the communication link (such as by placing a router within the neighboring entity's data center), then the Responsible Entity shall identify where the security protection is applied at both ends of the link. Similarly, if a Responsible Entity owns and operates both Control Centers which are exchanging data (such as in the case of a primary and backup Control Center), then the Responsible Entity shall identify where security protection is applied at both ends of the link.

Identification of ~~Roles and~~ Responsibilities when the Control Centers are Owned or Operated by Different Responsible Entities

The Technical Rationale and Justification for CIP-012-1 identifies key considerations in the Control Center Ownership section when communicationsing between Control Centers with different owners or operators. ~~Most if not all of the m~~Many operational relationships between Responsible Entities are unique. Consequently, there is no single way to identify ~~roles and~~ responsibilities for applying security protection to the transmission of Real-time Assessment and Real-time monitoring ~~and control~~ data between Control Centers.

Implementation of ~~Responsible Entities may consider identifying the roles and~~ responsibilities could also be demonstrated in many ways. ~~for the following situations: (1) configuration of security protocols, (2) responding to communication failures, and (3) responding to Cyber Security Incidents.~~ Some examples include a joint procedure, a memorandum of understanding, or meeting minutes between the two parties where responsibilities are ~~discussed~~defined.

~~General Considerations for R2~~

~~Given the format of the requirements, the majority of the documentation is required under R1 while R2 requires the implementation of the plan developed for R1. Compliance with R2 is established by implementing the protection identified in a Responsible Entity's R1 plan. The sections below outline examples of evidence that may be provided in order to demonstrate the implementation of Entity Alpha's CIP-012-1 R1 plan.~~

~~Identification of Security Protection~~

~~Implementation of the security protection can be demonstrated in many ways. If physical protection is used, a Responsible Entity may demonstrate implementation through a floor plan which identifies the physical security measures in place protecting the communication link. If logical protection is used, a Responsible Entity may demonstrate implementation through an export of the device configuration which applies the security protection. Alternatively, a Responsible Entity may demonstrate implementation through monitoring of the security control such as a report generated from an automated tool that monitors the encryption service used to protect a communications link.~~

~~Identification of Demarcation Point(s)~~

~~Identification of demarcation point(s) could be demonstrated with a diagram (physical or logical) or a list. This diagram or list could be included within the plan developed for R1. A label could also be used to identify a device as a demarcation point.~~

~~Identification of Roles and Responsibilities when the Control Centers are Owned or Operated by Different Responsible Entities~~

~~Implementation of roles and responsibilities could also be demonstrated in many ways. Some examples include a joint procedure, a memorandum of understanding or meeting minutes between the two parties where roles and responsibilities are discussed.~~

Reference Model~~s~~

For this Implementation Guidance, the SDT uses a basic reference model of Primary and Backup Control Centers (Entity Alpha) to illustrate approaches ~~concepts necessary~~ to demonstrating~~e~~ compliance. These Control Centers communicate to each other and to a neighboring entity's Control Center (Entity Beta) in configurations outlined by the diagrams in this section. The SDT recognizes that the reference model~~s~~ does not contain many of the complexities of a real Control Center. For this Implementation Guidance, the registration or functions performed in the reference model Control Center are also not considered. A high level block diagram of the basic reference model is shown below in Figure 1. This Implementation Guidance is developed from the perspective of Entity Alpha.

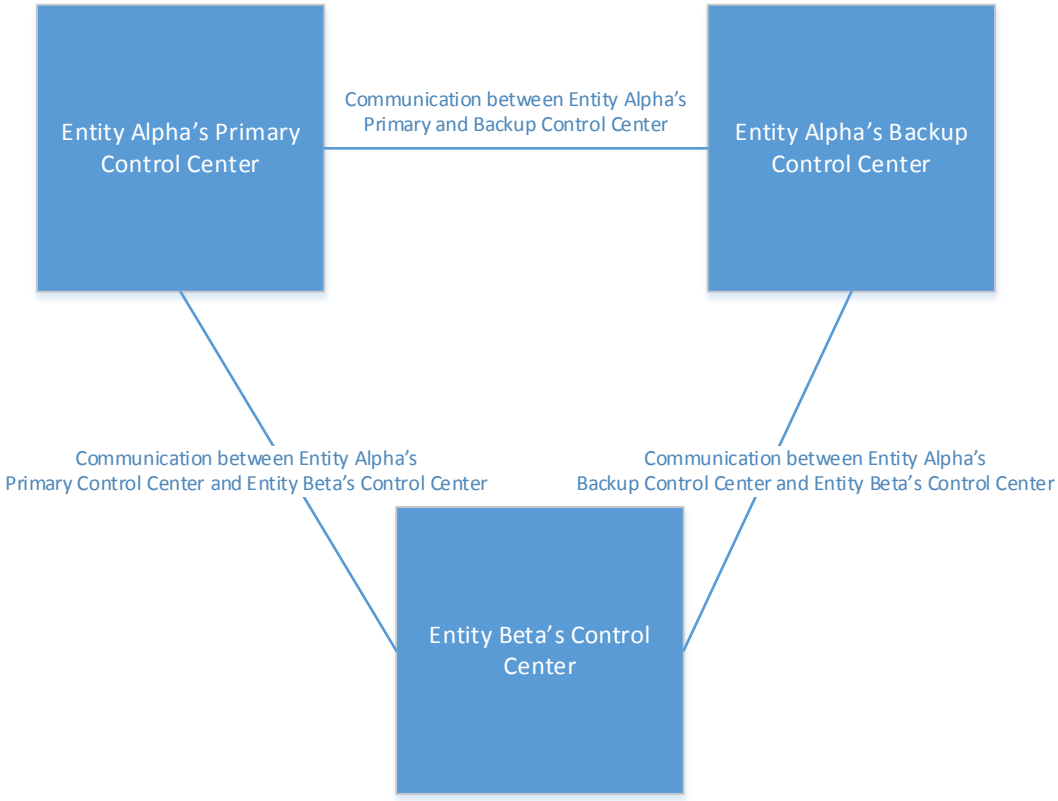


Figure 1: High Level Block Diagram of Reference Model Control Centers

Reference Model Discussion

Requirement R1 requires the implementation of a documented plan. To comply with requirement R1, one approach to a plan is to first determine which communications ~~require protection under~~ are in scope of CIP-012-1. There are multiple ways to identify an entity's scope in R1. For example, Entity Alpha in the reference model may first identify the Control Centers with which it communicates. Entity Alpha would determine that there are three: Entity Alpha's Primary Control Center, Entity Alpha's Backup Control Center, and Entity Beta's Control Center. Entity Alpha does not need to consider whether Entity Beta further shares its data with another Entity. That is the responsibility of Entity Beta and is outside of Entity Alpha's purview. Additionally, Entity Alpha does not need to consider any communications to other non-Control Center facilities such as generating plants or substations. These communications are out of scope for CIP-012-1.

Now that Entity Alpha has identified the Control Centers with which it communicates, Entity Alpha identifies either: (1) the Real-time Assessment and Real-time monitoring data; or (2) communication links which are used to transmit Real-time Assessment and Real-time monitoring data between Control Centers. In either case, Entity Alpha should refer to the data specification for Real-time Assessment and Real-time monitoring data identified

in TOP-003-3 and IRO-010-2. For this reference model scenario, identifying the communication links used to transmit Real-time Assessment and Real-time monitoring data may be the most straightforward approach. Through an evaluation of communication links between Control Centers and an evaluation of how it transmits and receives Real-time Assessment and Real-time monitoring data, Entity Alpha determined that it communicates applicable data between its primary and backup Control Centers across a single communication link. Entity Alpha also determined that it communicates applicable data to and from Entity Beta's Control Center across one of two links that originate from either Entity Alpha's primary or backup Control Center using the Inter-Control Center Communications Protocol (ICCP).

With an identified scope of communications links, Entity Alpha now considers the three required elements of its required communications between Control Centers for its plan.

Identification of Security Protection

- Entity Alpha must ensure that protection is applied where identified in its CIP-012-1 plan. The protection must also meet the security objective of mitigating the risk of unauthorized disclosure or modification of applicable data while in transit between Control Centers. The identification of security protection could be demonstrated by a network diagram similar to that shown in Figure 2 or Figure 3.
- In a simple case where the security protection is applied sufficiently close to the Control Center, such as within the Physical Security Perimeter of the Control Center, Entity Alpha may use a single security protection method to meet the security objective. For this case, shown in Figure 2, Entity Alpha implements a Virtual Private Network (VPN) connection across a private leased communication circuit for each of its three in-scope communication links. To meet the security objective, Entity Alpha further states that its VPN uses Internet Protocol security (IPsec) with encryption.
- For more complex scenarios, Entity Alpha may need to use a combination of security controls. For instance, in Figure 3, Entity Alpha uses a combination of physical security controls (physical access control) and logical security controls (encrypted communications consistent with the first scenario above) to meet the security objective.
- While these scenarios are all specific to communication links, it is possible that Entity Alpha and Entity Beta achieve the security objective by applying protection to the data rather than the communication links. In this scenario, the application enabling the data exchange between Control Centers may be capable of applying security controls directly to the data. These security controls mitigate the risk of unauthorized disclosure or modification of applicable data rather than relying on lower level network services to provide this security. For instance, Entity Alpha and Entity Beta may apply security protection at the application layer by using Secure ICCP to exchange applicable data. According to a report released by Sandia National Labs[2], Secure ICCP provides "data integrity indirectly by providing a cryptographic checksum. ~~...~~Secure ICCP provides data confidentiality by encrypting ICCP data exchanges." Methods other than Secure ICCP could also be used to apply security protection to the data at the application layer.
- It is theoretically possible that Entity Alpha and Entity Beta could exchange Real-time Assessment data between Control Centers by email. In that scenario, one approach may be for Entity Alpha to email the applicable data to Entity Beta's Control Center in a protected container such as an encrypted zip file. Entity Alpha and Entity Beta can then exchange the password to that encrypted container through another method, such as by phone. While the notional example of protecting data exchanged by email is a useful illustration of how to achieve the security objective of CIP-012-1, it is extremely unlikely to be used in practice. The characteristics of email communication are inconsistent with the requirements of Real-time data exchange.

[2] https://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/19-Secure_ICCP_Integration.pdf

-Identification of Where Security Protection is Applied by the Responsible Entity

Similar to the identification of security protection above, the identification of where security protection is applied can also be demonstrated by a network diagram similar to those found in Figures 2 and 3.

- Figure 2 shows the identification where CIP-012-1 security protection is applied for the Entity Alpha reference model when a single encrypted tunnel is used to implement the required protection. Entity Alpha has identified that security protection is applied at each of its Control Centers on the external Ethernet interface on the WAN router. While the diagram depicts where Entity Beta has applied security protection for illustrative purposes, Entity Alpha is not responsible for identifying where Entity Beta has applied security protection.

- In ~~some cases~~ order to understand the application of security protection in context of who controls the communication link, it may be helpful to identify both where CIP-012-1 security protection is applied and the location of the telecommunications carrier (telco) demarcation point. Figure 3 provides such an example where the telco demarcation point may not be within the Control Center and based the facts and circumstances surrounding this scenario, Entity Alpha has implemented a combination of security controls to comply with CIP-012-1. In this scenario, Entity Alpha identifies that it has applied physical security protection for its PSP and continuing for its WAN router and that it has applied logical security protection (encryption) at the WAN router. Entity Alpha has also identified the telco demarcation point at a point in the telecommunications cabling connecting to Entity Alpha's WAN router, perhaps at a punch down block for example. In Figure 3, the telco demarcation point is inside the same room as the WAN router. The telco demarcation points are referenced in the drawing for clarity, but are not part of the plan.

- The data-centric scenario described above is less intuitive for identifying where security protection is applied by Entity Alpha. If security protection is applied at the application layer (such as Secure ICCP), Entity Alpha could reasonably identify the application or service applying the security (such as the Secure ICCP service) as the location of where security protection is applied.

Identification of Responsibilities when the Control Centers are Owned or Operated by Different Responsible Entities

Entity Alpha and Entity Beta may determine they each are responsible for one end of the VPN configuration on their respective WAN routers. Entity Alpha and Entity Beta have agreed to a 30 character pre-shared key for IPSec authentication.

Rather than use a pre-shared key, Entity Alpha and Entity Beta may decide to use digital certificates for the IPSec authentication using a trusted certificate authority. In that scenario, Entity Alpha and Entity Beta would agree on who is the party responsible for managing the certificate authority.

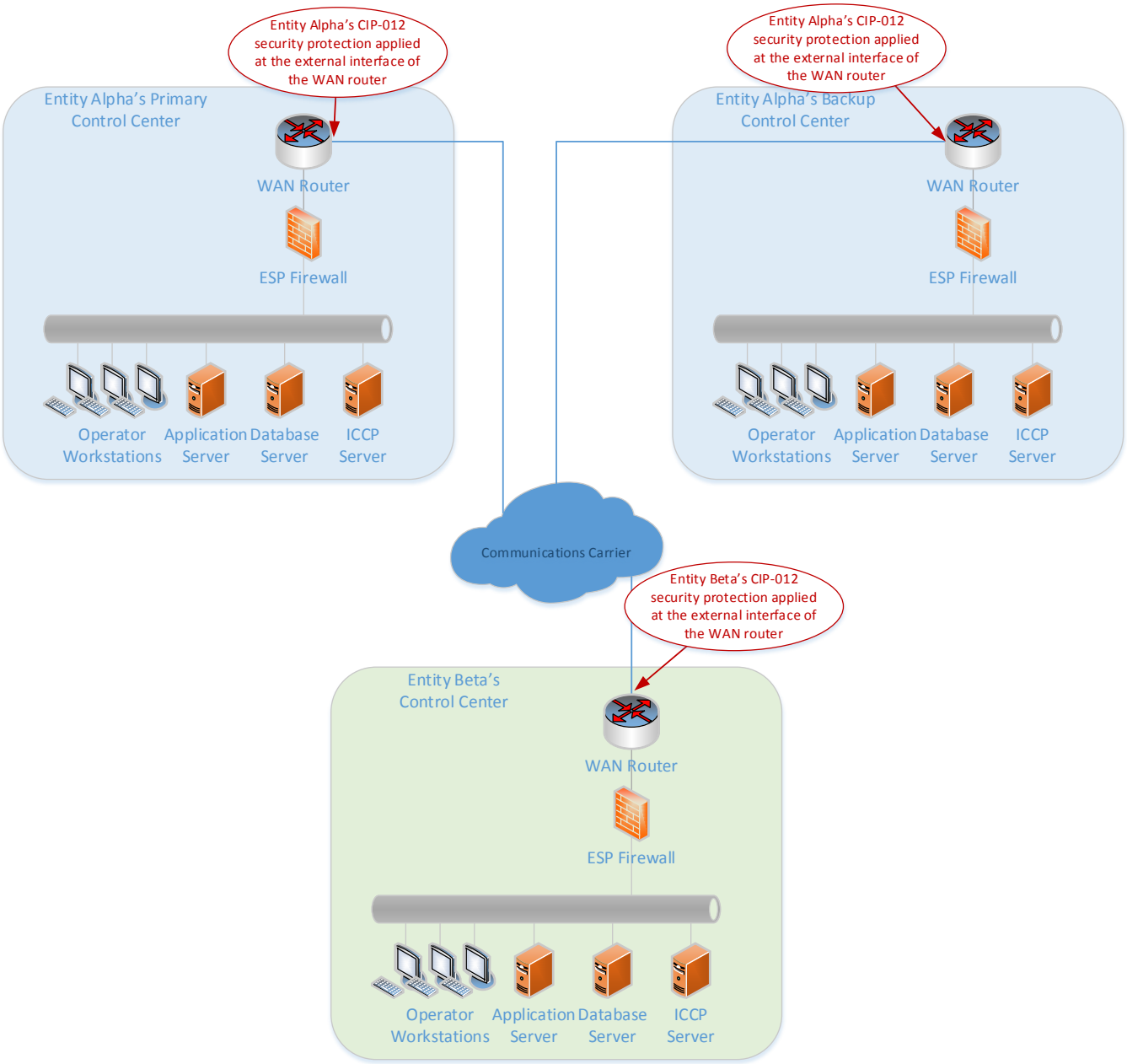


Figure 2: Network diagram and identification of where security protection is applied

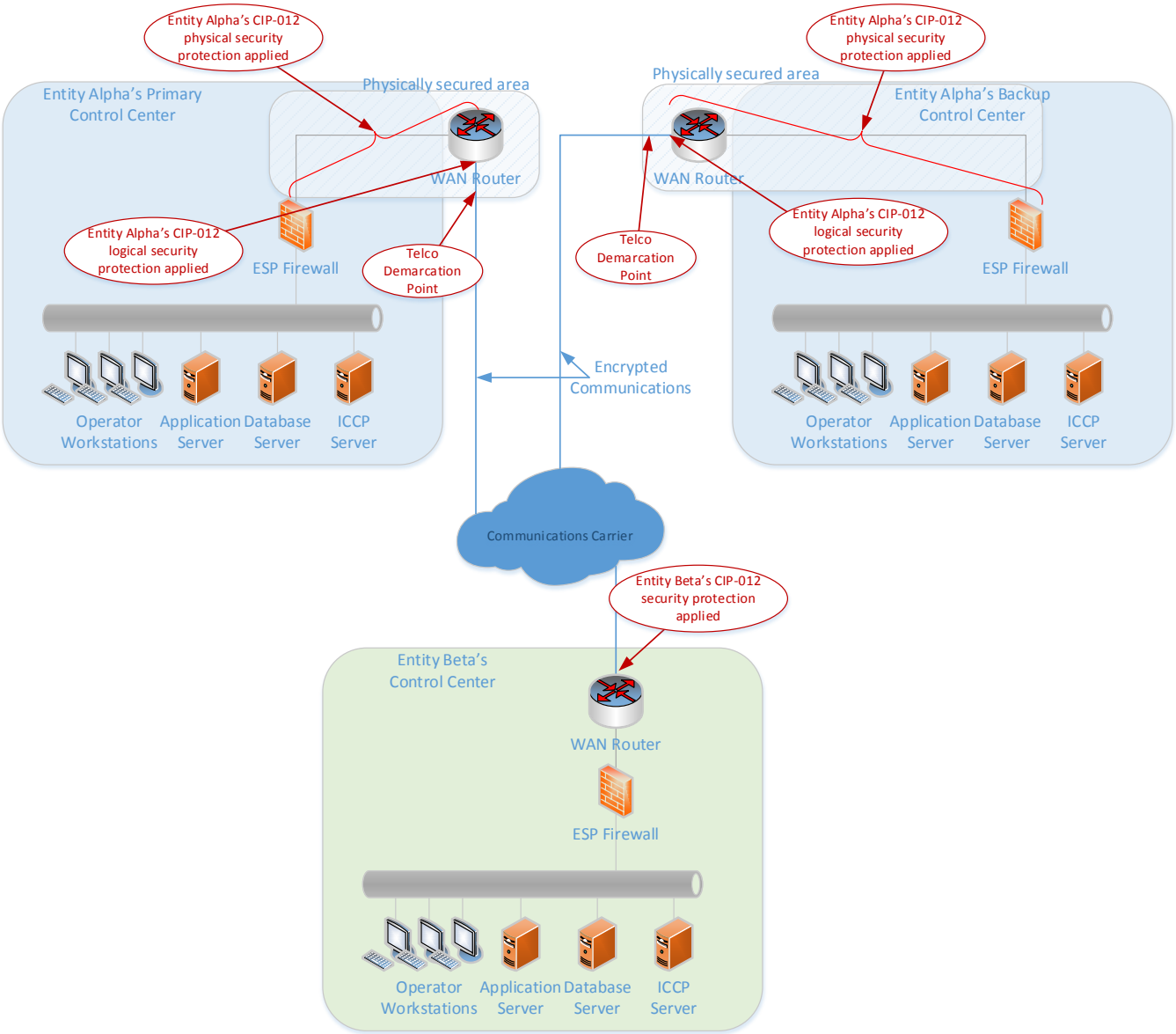


Figure 3: Network diagram using a combination of controls for CIP-012-1

References

Mitre Common Weakness Enumeration (CWE™) list of software weakness types
https://cwe.mitre.org/data/definitions/327.html

Cryptographic Standards and Guidelines
https://csrc.nist.gov/Projects/Cryptographic-Standards-and-Guidelines

NIST Special Publication 800-175B
Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-175B.pdf

Guide to Cryptography
https://www.owasp.org/index.php/Guide_to_Cryptography#Symmetric_Cryptography

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DRAFT

Cyber Security – Communications between Control Centers

Technical Rationale and Justification for Reliability Standard CIP-012-1

March 2018

RELIABILITY | ACCOUNTABILITY



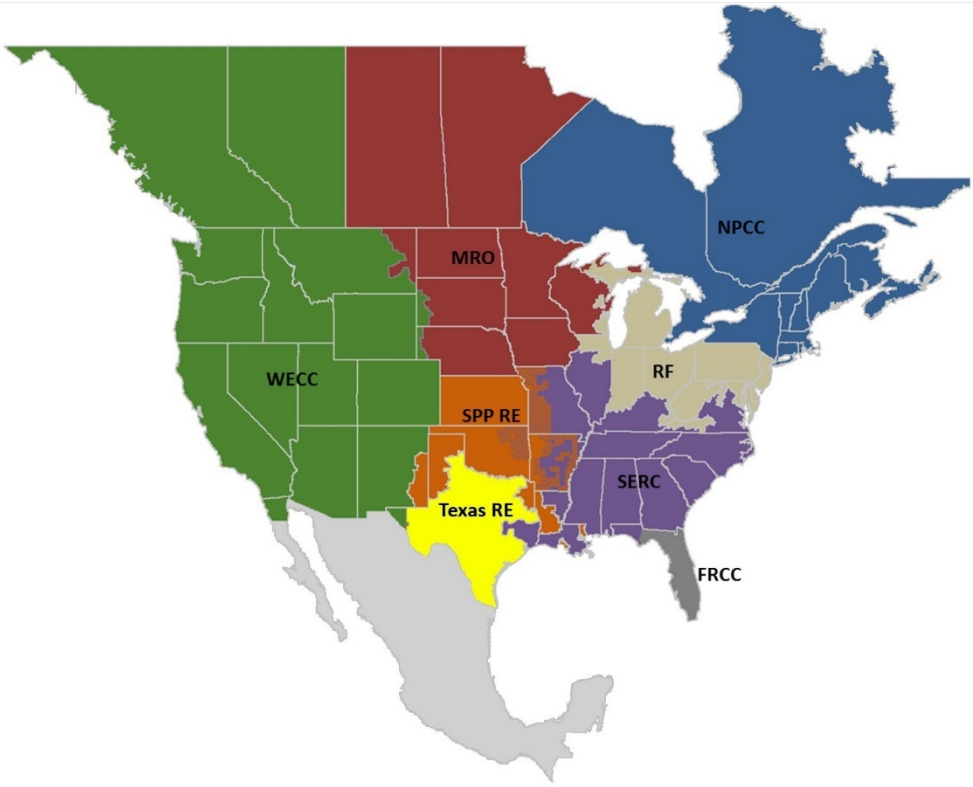

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Preface

The vision for the Electric Reliability Organization (ERO) Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the eight Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

The North American BPS is divided into eight RE boundaries as shown in the map and corresponding table below.



The North American BPS is divided into eight RE boundaries. The highlighted areas denote overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.

FRCC	Florida Reliability Coordinating Council
MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
SPP RE	Southwest Power Pool Regional Entity
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-012-1. It will provide stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. It also contains information on the SDT's intent in drafting the requirements. This Technical Rationale and Justification for CIP-012-1 is not a Reliability Standard and should not be considered mandatory and enforceable.

On January 21, 2016, the Federal Energy Regulatory Commission (FERC or Commission) issued Order No. 822, approving seven Critical Infrastructure Protection (CIP) Reliability Standards and new or modified terms in the Glossary of Terms Used in NERC Reliability Standards, and directing modifications to the CIP Reliability Standards. Among others, the Commission directed the North American Electric Reliability Corporation (NERC) to "develop modifications to the CIP Reliability Standards to require Responsible Entities[1] to implement controls to protect, at a minimum, communication links and sensitive bulk electric system data communicated between bulk electric system Control Centers in a manner that is appropriately tailored to address the risks posed to the bulk electric system by the assets being protected (i.e., high, medium, or low impact)." (Order 822, Paragraph 53)

In response to the directive in Order No. 822, the Project 2016-02 standard drafting team (SDT) drafted Reliability Standard CIP-012-1 to require Responsible Entities to implement controls to protect sensitive Bulk Electric System (BES) data and communications links between BES Control Centers. Due to the sensitivity of the data being communicated between Control Centers, as defined in the Glossary of Terms Used in NERC Reliability Standards, the standard applies to all impact levels (i.e., high, medium, or low impact).

Although the Commission directed NERC to develop modifications to CIP-006, the SDT determined that modifications to CIP-006 would not be appropriate. There are differences between the plan(s) required to be developed and implemented for CIP-012-1 and the protection required in CIP-006-6 Requirement R1 Part 1.10. CIP-012-1 Requirements R1 and R2 protect the applicable data during transmission between two separate Control Centers. CIP-006 Requirement R1 Part 1.10 protects nonprogrammable communication components within an Electronic Security Perimeter (ESP) but outside of a Physical Security Perimeter (PSP). The transmission of applicable data between Control Centers takes place outside of an ESP. Therefore, the protection contained in CIP-006-6 Requirement R1 Part 1.10 does not apply.

The SDT drafted requirements to provide Responsible Entities the latitude to protect the communication links, the data, or both to satisfy the security objective consistent with the capabilities of the Responsible Entity's operational environment.

[1] As used in the CIP Standards, a Responsible Entity refers to the registered entities subject to the CIP Standards.

Requirement R1

R1. The Responsible Entity shall implement one or more documented plan(s) to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring data while being transmitted between any Control Centers. This requirement excludes oral communications. The plan shall include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1 *Identification of security protection used to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring while being transmitted between Control Centers;*

1.2 *Identification of where the Responsible Entity applied security protection for transmitting Real-time Assessment and Real-time monitoring data between Control Centers; and*

1.3 *If the Control Centers are owned or operated by different Responsible Entities, identify the responsibilities of each Responsible Entity for applying security protection to the transmission of Real-time Assessment and Real-time monitoring data between those Control Centers.*

General Considerations for Requirement R1

Requirement R1 focuses on implementing a document plan to protect information that is critical to the Real-time operations of the Bulk Electric System while in transit between applicable Control Centers. The SDT does not intend for the listed order of the three requirement parts to convey any sequence or significance.

Overview of confidentiality and integrity

The SDT drafted CIP-012-1 to address confidentiality and integrity of Real-time Assessment and Real-time monitoring data. This is accomplished by drafting the requirement to mitigate the risk of unauthorized disclosure (confidentiality) or modification (integrity). For this Standard, the SDT relied on the definitions of confidentiality and integrity as defined by National Institute of Standards and Technology (NIST):

- Confidentiality is defined as, "Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information."[2]
- Integrity is defined as, "Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity."[3]

The SDT asserts that the availability of this data is already required by the performance obligation of the Operating and Planning Reliability Standards. The SDT drafted CIP-012 to address the data while being transmitted. The SDT maintains that this data resides within BES Cyber Systems, and while at rest is protected by CIP-003 through CIP-011.

Alignment with IRO and TOP standards

The SDT recognized the FERC reference to additional Reliability Standards and the responsibilities to protect the applicable data in accordance with NERC Reliability Standards TOP-003 and IRO-010. The SDT used these references to drive the identification of sensitive BES data and chose to base the CIP-012 requirements on the Real-time data specification elements in these standards. This approach provides consistent scoping of identified data, and does not require each entity to devise its own list or inventory of this data. Many entities are required to provide this data under agreements executed with their RC, BA or TOP. The SDT asserts that typically the RC, BA or TOP will identify all data requiring protection for CIP-012-1 through the TOP-003 and IRO-010 Reliability Standards. However, the SDT

[2] NIST Special Publication 800-53A, Revision 4, page B-3
[3] NIST Special Publication 800-53A, Revision 4, page B-6

noted that there may be special instances during which Real-time Assessment or Real-time Monitoring data is not identified by the RC, BA, or TOP. This would include data that may be exchanged between a Responsible Entity's primary and backup Control Center.

Identification of Where Security Protection is Applied by the Responsible Entity

The SDT noted the need for a Responsible Entity to identify where it will apply protection for applicable data. The SDT did not specify the location where CIP-012 security protection must be applied to provide latitude for Responsible Entities to implement the security controls in a manner best fitting their individual circumstances. This latitude ensures entities can still take advantage of security measures, such as deep packet inspection implemented at or near the EAP when ESPs are present, while maintaining the capability to protect the applicable data being transmitted between Control Centers.

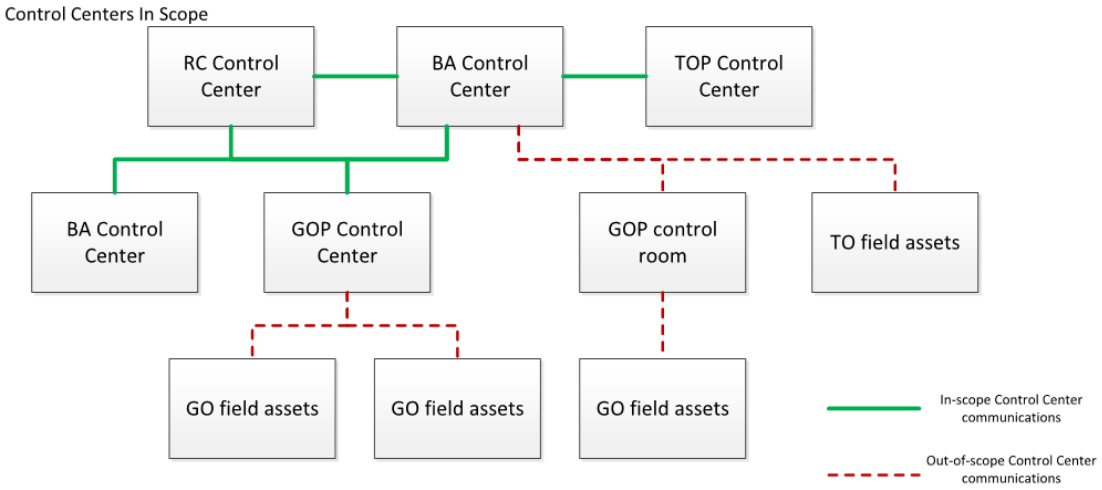
The SDT also recognizes that CIP-012 security protection may be applied to a Cyber Asset that is not an identified BES Cyber Asset or EACMS. The identification of the Cyber Asset as the location where security protection is applied does not expand the scope of Cyber Assets identified as applicable under Cyber Security Standards CIP-002 through CIP-011.

The SDT understands that in data exchanges between Control Centers, a single entity may not be responsible for both ends of the communication link. The SDT intends for a Responsible Entity to identify only where it applied security protection. The Responsible Entity should not be held accountable for identifying where a neighboring entity applied security protection at the neighboring entity's facility. A Responsible Entity, however, may decide to take responsibility for both ends of a communication link. For example, it may place a router in a neighboring entity's data center. In a scenario like this, where a Responsible Entity has taken responsibility for applying security protection on both ends of the communication link, the Responsible Entity should identify where it applied security protection at both ends of the link. The SDT intends for there to be alignment between the identification of where security protection is applied in CIP-012 R1, Part 1.2 and the identification of Responsible Entity responsibilities in CIP-012 R1, Part 1.3.

Control Center Ownership

The requirements address protection for Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers owned by a single Responsible Entity. They also cover the applicable data transmitted between Control Centers owned by two or more separate Responsible Entities. Unlike protection between a single Responsible Entity's Control Centers, applying protection between Control Centers owned by more than one Responsible Entity requires additional coordination. The requirements do not explicitly require formal agreements between Responsible Entities partnering for protection of applicable data. It is strongly recommended, however, that these partnering entities develop agreements, or use existing ones, to define responsibilities to ensure the security objective is met. An example noted in FERC Order No. 822 Paragraph 59 is, "if several registered entities have joint responsibility for a cryptographic key management system used between their respective Control Centers, they should have the prerogative to come to a consensus on which organization administers that particular key management system."

As an example, the reference model below shows some of the data transmissions between Control Centers that a Responsible Entity should consider to be in-scope. The example does not include all possible scenarios. The solid green lines are in-scope communications. The dashed red lines are out-of-scope communications.



This reference model is an example and does not include all possible scenarios.

References

Here are several references to assist entities in developing plan(s) for protection of communication links:

- NIST Special Publication 800-53A, Revision 4: Security and Privacy Controls for Federal Information Systems and Organizations
- NIST Special Publication 800-82: Guide to Industrial Control Systems (ICS) Security
- NIST Special Publication 800-175B: Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms
- NIST Special Publication 800-47: Security Guide for Interconnecting Information Technology Systems

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DRAFT

Cyber Security – Communications between Control Centers

Technical Rationale and Justification for Reliability Standard CIP-012-1

~~November~~ March 2018~~7~~

RELIABILITY | ACCOUNTABILITY



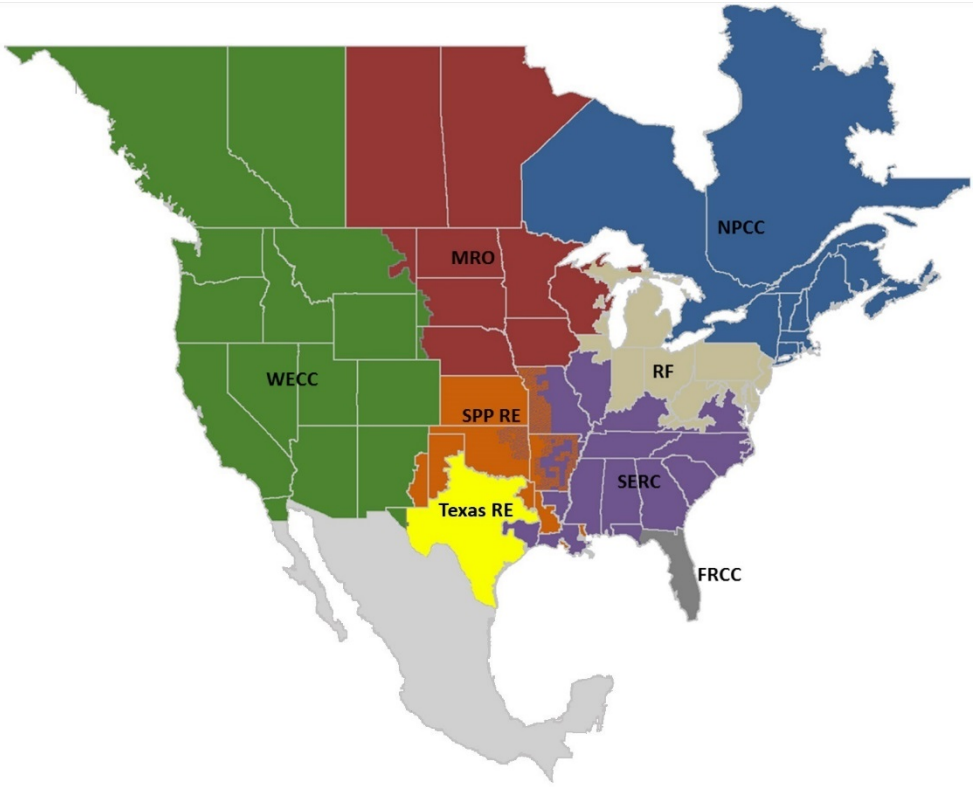

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Preface

The vision for the Electric Reliability Organization (ERO) Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the eight Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

The North American BPS is divided into eight RE boundaries as shown in the map and corresponding table below.



The North American BPS is divided into eight RE boundaries. The highlighted areas denote overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.

FRCC	Florida Reliability Coordinating Council
MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
SPP RE	Southwest Power Pool Regional Entity
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-012-1. It will provide stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. It also contains information on the SDT's intent in drafting the requirements. This Technical Rationale and Justification for CIP-012-1 is not a Reliability Standard and should not be considered mandatory and enforceable.

On January 21, 2016, the Federal Energy Regulatory Commission (FERC or Commission) issued Order No. 822, approving seven Critical Infrastructure Protection (CIP) Reliability Standards and new or modified terms in the Glossary of Terms Used in NERC Reliability Standards, and directing modifications to the CIP Reliability Standards. Among others, the Commission directed the North American Electric Reliability Corporation (NERC) to "develop modifications to the CIP Reliability Standards to require Responsible Entities[1] to implement controls to protect, at a minimum, communication links and sensitive bulk electric system data communicated between bulk electric system Control Centers in a manner that is appropriately tailored to address the risks posed to the bulk electric system by the assets being protected (i.e., high, medium, or low impact)." (Order 822, Paragraph 53)

In response to the directive in Order No. 822, the Project 2016-02 standard drafting team (SDT) drafted Reliability Standard CIP-012-1 to require Responsible Entities to implement controls to protect sensitive Bulk Electric System (BES) data and communications links between BES Control Centers. Due to the sensitivity of the data being communicated between Control Centers, as defined in the Glossary of Terms Used in NERC Reliability Standards, the standard applies to all impact levels (i.e., high, medium, or low impact).

Although the Commission directed NERC to develop modifications to CIP-006, the SDT determined that modifications to CIP-006 would not be appropriate. There are differences between the plan(s) required to be developed and implemented for CIP-012-1 and the protection required in CIP-006-6 Requirement R1 Part 1.10. CIP-012-1 Requirements R1 and R2 protect the applicable data during transmission between two separate Control Centers. CIP-006 Requirement R1 Part 1.10 protects nonprogrammable communication components within an Electronic Security Perimeter (ESP) but outside of a Physical Security Perimeter (PSP). The transmission of applicable data between Control Centers takes place outside of an ESP. Therefore, the protection contained in CIP-006-6 Requirement R1 Part 1.10 does not apply.

The SDT drafted requirements to provide Responsible Entities the latitude to protect the communication links, the data, or both to satisfy the security objective consistent with the capabilities of the Responsible Entity's operational environment. ~~Requirement R1 requires Responsible Entities to implement one or more documented plan(s) that protect Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers. The plan(s) must address how the Responsible Entity will mitigate the risk of unauthorized disclosure or modification of the applicable data.~~

[1] As used in the CIP Standards, a Responsible Entity refers to the registered entities subject to the CIP Standards.

Requirement R1

R1. The Responsible Entity shall ~~develop~~ implement one or more documented plan(s) to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring ~~and control~~ data while being transmitted between any Control Centers. This requirement excludes oral communications. The plan shall include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1 *Identification of security protection used to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring ~~and control data~~ while being transmitted between Control Centers;*

1.2 *Identification of ~~demarcation point(s)~~ where the Responsible Entity applied security protection ~~is applied~~ for transmitting Real-time Assessment and Real-time monitoring ~~and control~~ data between Control Centers; and*

1.3 *If ~~Identification of roles and responsibilities of each Responsbile Entity for applying security protection to the transmission of Real-time Assessmsnet and Real-time monitoring and control data between Control Centers, when t~~he Control Centers are owned or operated by different Responsible Entities,identify the responsibilities of each Responsible Entity for applying security protection to the transmission of Real-time Assessment and Real-time monitoring data between those Control Centers.*

General Considerations for Requirement R1

Requirement R1 focuses on ~~developing~~ implementing a document plan to protect information that is critical to the ~~real~~Real-time operations of the Bulk Electric System while in transit between applicable Control Centers. The SDT does not intend for the listed order of the three requirement parts to convey any sequence or significance.

Overview of confidentiality and integrity

The SDT drafted CIP-012-1 to address confidentiality and integrity of Real-time Assessment and Real-time monitoring ~~and Control~~ data. This is accomplished by drafting the requirement to mitigate the risk of unauthorized disclosure (confidentiality) or modification (integrity). For this Standard, the SDT relied on the definitions of confidentiality and integrity as defined by National Institute of Standards and Technology (NIST):

- Confidentiality is defined as, "Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information."[2]
- Integrity is defined as, "Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity."[3]

The SDT asserts that the availability of this data is already required by the performance obligation of the Operating and Planning Reliability Standards. The SDT drafted CIP-012 to address the data while being transmitted. The SDT maintains that this data resides within BES Cyber Systems, and while at rest is protected by CIP-003 through CIP-011.

Alignment with IRO and TOP standards

The SDT recognized the FERC reference to additional Reliability Standards and the responsibilities to protect the applicable data in accordance with NERC Reliability Standards TOP-003 and IRO-010. The SDT used these references

[2] NIST Special Publication 800-53A, Revision 4, page B-3
[3] NIST Special Publication 800-53A, Revision 4, page B-6

to drive the identification of sensitive BES data and chose to base the CIP-012 requirements on the Real-time data specification elements in these standards. This approach provides consistent scoping of identified data, and does not require each entity to devise its own list or inventory of this data. Many entities are required to provide this data under agreements executed with their RC, BA or TOP~~., often without benfit of knowing how those entities use that data. The SDT notes that it expanded the phrase "Real-time monitoring" data from TOP-003 and IRO-010 to "Real-time monitoring and control" data. The SDT was concerned that data transmitted between Control Centers that results in the physical operation of BES Elements was not explicitly included in Real-time monitoring data. The SDT understands that in practice Real-time control data is not transmitted separately from Real-time monitoring data. However, the SDT wanted to ensure that Real-time control data was included regardless of whether or not it is transmitted along with Real-time monitoring data. If entities only transmit Real-time control data along with Real-time monitoring data, then the SDT does not intend for such entities to identify additional data beyond that Real-time monitoring data already included in the data specifications for TOP-003 and IRO-010.~~ The SDT asserts that typically the RC, BA or TOP will identify all data requiring protection for CIP-012-1 through the TOP-003 and IRO-010 Reliability Standards. However, the SDT noted that there may be special instances during which Real-time Assessment or Real-time Monitoring data is not identified by the RC, BA, or TOP. This would include data that may be exchanged between a Responsible Entity's primary and backup Control Center.

~~Demarcation Points~~

~~The SDT noted the need for an entity to identify a demarcation point inside each Control Center where it will apply protection for applicable data. The SDT used the demarcation point concept for implementing protection to ensure entities could still take advantage of security measures, such as deep packet inspection, already implemented at or near the EAP when ESPs are present, while maintaining the capability to protect the applicable data being transmitted between Control Centers.~~

Identification of Where Security Protection is Applied by the Responsible Entity

The SDT noted the need for a Responsible Entity to identify where it will apply protection for applicable data. The SDT did not specify the location where CIP-012 security protection must be applied to provide latitude for Responsible Entities to implement the security controls in a manner best fitting their individual circumstances. This latitude ensures entities can still take advantage of security measures, such as deep packet inspection implemented at or near the EAP when ESPs are present, while maintaining the capability to protect the applicable data being transmitted between Control Centers.

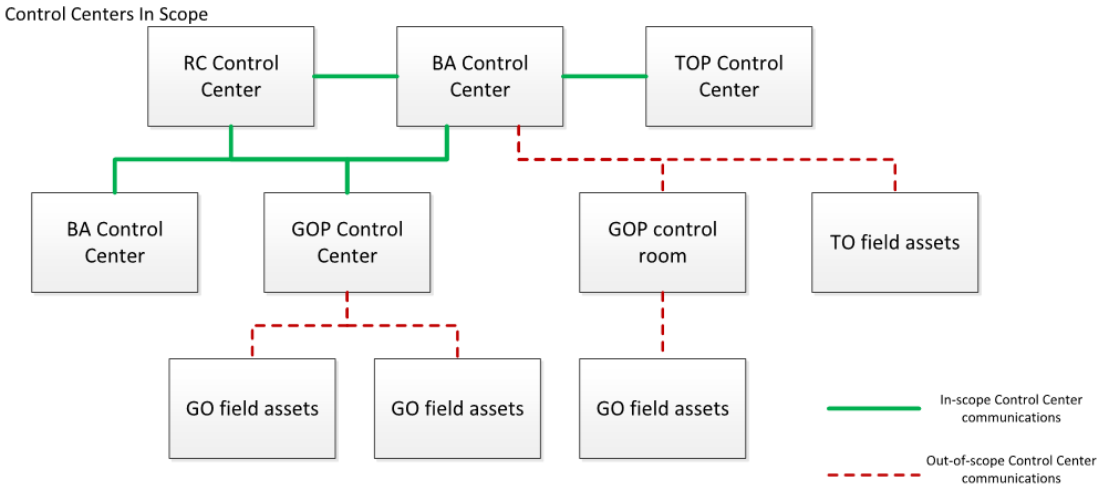
The SDT also recognizes that CIP-012 security protection may be applied to a Cyber Asset that is not an identified BES Cyber Asset or EACMS. The identification of the Cyber Asset as the location where security protection is applied does not expand the scope of Cyber Assets identified as applicable under ~~the CIP~~ Cyber Security Standards CIP-002 through CIP-011.

The SDT understands that in data exchanges between Control Centers, a single entity may not be responsible for both ends of the communication link. The SDT intends for a Responsible Entity to identify only where it applied security protection. The Responsible Entity should not be held accountable for identifying where a neighboring entity applied security protection at the neighboring entity's facility. A Responsible Entity, however, may decide to take responsibility for both ends of a communication link. For example, it may place a router in a neighboring entity's data center. In a scenario like this, where a Responsible Entity has taken responsibility for applying security protection on both ends of the communication link, the Responsible Entity should identify where it applied security protection at both ends of the link. The SDT intends for there to be alignment between the identification of where security protection is applied in CIP-012 R1, Part 1.2 and the identification of Responsible Entity responsibilities in CIP-012 R1, Part 1.3.

Control Center Ownership

The requirements address protection for Real-time Assessment and Real-time monitoring ~~and control~~ data while being transmitted between Control Centers owned by a single Responsible Entity. They also cover the applicable data transmitted between Control Centers owned by two or more separate Responsible Entities. Unlike protection between a single Responsible Entity's Control Centers, applying protection between Control Centers owned by more than one Responsible Entity requires additional coordination. The requirements do not explicitly require formal agreements between Responsible Entities partnering for protection of applicable data. It is strongly recommended, however, that these partnering entities develop agreements, or use existing ones, to define responsibilities to ensure ~~adequate protection is applied~~ the security objective is met. An example noted in FERC Order No. 822 Paragraph 59 is, "if several registered entities have joint responsibility for a cryptographic key management system used between their respective Control Centers, they should have the prerogative to come to a consensus on which organization administers that particular key management system."

As an example, the reference model below ~~depicts~~ shows some of the data transmissions between Control Centers that a Responsible Entity should consider to be in-scope. The example does not include all possible scenarios. The solid green lines are in-scope communications. The dashed red lines are out-of-scope communications.



This reference model is an example and does not include all possible scenarios.

References

Here are several references to assist entities in developing plan(s) for protection of communication links:

- NIST Special Publication 800-53A, Revision 4: Security and Privacy Controls for Federal Information Systems and Organizations
- NIST Special Publication 800-82: Guide to Industrial Control Systems (ICS) Security
- NIST Special Publication 800-175B: Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms
- NIST Special Publication 800-47: Security Guide for Interconnecting Information Technology Systems

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Reliability Standard Audit Worksheet[1]

CIP-012-1 – Cyber Security – Communications between Control Centers

This section to be completed by the Compliance Enforcement Authority.

Audit ID:	Audit ID if available; or REG-NCRnnnnn-YYYYMMDD
Registered Entity:	Registered name of entity being audited
NCR Number:	NCRnnnnn
Compliance Enforcement Authority:	Region or NERC performing audit
Compliance Assessment Date(s)[2]:	Month DD, YYYY, to Month DD, YYYY
Compliance Monitoring Method:	[On-site Audit | Off-site Audit | Spot Check]
Names of Auditors:	Supplied by CEA

Applicability of Requirements

	BA	DP	GO	GOP	PA/PC	RC	RP	RSG	TO	TOP	TP	TSP
R1	X		X	X		X			X	X		

Legend:

Text with blue background:	Fixed text – do not edit
Text entry area with Green background:	Entity-supplied information
Text entry area with white background:	Auditor-supplied information

[1] NERC developed this Reliability Standard Audit Worksheet (RSAW) language in order to facilitate NERC's and the Regional Entities' assessment of a registered entity's compliance with this Reliability Standard. The NERC RSAW language is written to specific versions of each NERC Reliability Standard. Entities using this RSAW should choose the version of the RSAW applicable to the Reliability Standard being assessed. While the information included in this RSAW provides some of the methodology that NERC has elected to use to assess compliance with the requirements of the Reliability Standard, this document should not be treated as a substitute for the Reliability Standard or viewed as additional Reliability Standard requirements. In all cases, the Regional Entity should rely on the language contained in the Reliability Standard itself, and not on the language contained in this RSAW, to determine compliance with the Reliability Standard. NERC's Reliability Standards can be found on NERC's website. Additionally, NERC Reliability Standards are updated frequently, and this RSAW may not necessarily be updated with the same frequency. Therefore, it is imperative that entities treat this RSAW as a reference document only, and not as a substitute or replacement for the Reliability Standard. It is the responsibility of the registered entity to verify its compliance with the latest approved version of the Reliability Standards, by the applicable governmental authority, relevant to its registration status.

The RSAW may provide a non-exclusive list, for informational purposes only, of examples of the types of evidence a registered entity may produce or may be asked to produce to demonstrate compliance with the Reliability Standard. A registered entity's adherence to the examples contained within this RSAW does not necessarily constitute compliance with the applicable Reliability Standard, and NERC and the Regional Entity using this RSAW reserve the right to request additional evidence from the registered entity that is not included in this RSAW. This RSAW may include excerpts from FERC Orders and other regulatory references which are provided for ease of reference only, and this document does not necessarily include all applicable Order provisions. In the event of a discrepancy between FERC Orders, and the language included in this document, FERC Orders shall prevail.

[2] Compliance Assessment Date(s): The date(s) the actual compliance assessment (on-site audit, off-site spot check, etc.) occurs.

Findings

(This section to be completed by the Compliance Enforcement Authority)

Req.	Finding	Summary and Documentation	Functions Monitored
R1			

Req.	Areas of Concern

Req.	Recommendations

Req.	Positive Observations

Subject Matter Experts

Identify the Subject Matter Expert(s) responsible for this Reliability Standard.

Registered Entity Response (Required; Insert additional rows if needed):

SME Name	Title	Organization	Requirement(s)

Registered Entity Response (Required):

Question 1: Does the Registered Entity own or operate a Control Center? ☐ Yes ☐ No

If no:

1. Provide evidence in the space that the Registered Entity does not own or operate one or more Control Centers. This evidence may include, but is not limited to:
   - Evidence that the Registered Entity does not own or operate a Control Center; or
   - Evidence or a reference to evidence from the Registered Entity's CIP-002 compliance program that demonstrates the entity does not own or operate a Control Center.
2. The remainder of this RSAW may be left blank.

[Note: A separate spreadsheet or other document may be used. If so, provide the document reference below.]

R1 Supporting Evidence and Documentation

R1. The Responsible Entity shall implement one or more documented plan(s) to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring data while being transmitted between any Control Centers. This requirement excludes oral communications. The plan shall include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1 Identification of security protection used to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers;

1.2 Identification of where the Responsible Entity applied security protection for transmitting Real-time Assessment and Real-time monitoring data between Control Centers; and

1.3 If the Control Centers are owned or operated by different Responsible Entities, identify the responsibilities of each Responsible Entity for applying security protection to the transmission of Real-time Assessment and Real-time monitoring data between those Control Centers.

M1. Evidence may include, but is not limited to, documented plan(s) that meet the security objective of Requirement R1 and documentation demonstrating the implementation of the plan(s).

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-012-1, R1

This section to be completed by the Compliance Enforcement Authority

	If the Registered Entity has answered "No" to Question 1, verify the Registered Entity does not own or operate a Control Center. Note: If the Registered Entity does not own or operate a Control Center, the remainder of this RSAW is not applicable.
	Verify the entity has implemented one or more documented plan(s) to mitigate the risk of the unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers.
	Verify the documented plans collectively include identification of security protection used to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers.
	Verify the documented plans collectively include identification of where the Responsible Entity applied security protection for transmitting Real-time Assessment and Real-time monitoring data between Control Centers.
	Verify the documented plans collectively include identification of responsibilities of each Responsible Entity for applying security protection to the transmission of Real-time Assessment and Real-time monitoring data between Control Centers, when the Control Centers are owned or operated by different Responsible Entities.
	Verify the documented plans collectively achieve the security objective of mitigating the risk of the unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers.
Note to Auditor: 1. Oral communications are not in scope for CIP-012-1.	

Auditor Notes:

Additional Information:

Reliability Standard

The full text of CIP-012-1 may be found on the NERC Web Site (www.nerc.com) under "Program Areas & Departments", "Standards," "Reliability Standards."

In addition to the Reliability Standard, there is an applicable Implementation Plan available on the NERC Web Site.

In addition to the Reliability Standard, there is background information available on the NERC Web Site.

Capitalized terms in the Reliability Standard refer to terms in the NERC Glossary, which may be found on the NERC Web Site.

Sampling Methodology

Sampling is essential for auditing compliance with NERC Reliability Standards since it is not always possible or practical to test 100% of either the equipment, documentation, or both, associated with the full suite of enforceable standards. The Sampling Guide contained in the Compliance Monitoring and Enforcement Manual (see NERC website) provided by the Electric Reliability Organization help to establish a minimum sample set for monitoring and enforcement uses in audits of NERC Reliability Standards.

Regulatory Language

FERC Order 822 P53-56, 58, and 62

Selected Glossary Terms

The following Glossary terms are provided for convenience only. Please refer to the NERC web site for the current enforceable terms.

Control Center

One or more facilities, including their associated data centers, that monitor and control the Bulk Electric System (BES) and also host operating personnel who:

1) perform the Real-time reliability-related tasks of a Reliability Coordinator; or
2) perform the Real-time reliability-related tasks of a Balancing Authority; or
3) perform the Real-time reliability-related tasks of a Transmission Operator for Transmission Facilities at two or more locations; or
4) can act independently as the Generator Operator to develop specific dispatch instructions for generation Facilities at two or more locations; or
5) can operate or direct the operation of a Transmission Owner's BES Transmission Facilities in Real-time.

Operating personnel do not include:

1) plant operators located at a generator plant site or personnel at a centrally located dispatch center who relay dispatch instructions without making any modifications; or
2) Transmission Owner or Transmission Operator field switching personnel.

Real-time Assessment

An evaluation of system conditions using Real-time data to assess existing (pre-Contingency) and potential (post-Contingency) operating conditions. The assessment shall reflect applicable inputs including, but not limited to: load, generation output levels, known Protection System and Special Protection System status or degradation, Transmission outages, generator outages, Interchange, Facility Ratings, and identified phase angle and equipment limitations. (Real-time Assessment may be provided through internal systems or through third-party services.)

Real-time

Present time as opposed to future time.

Revision History for RSAW

Version	Date	Reviewers	Revision Description
Draft1 v1	07/28/2017	NERC Stds Group	New document
Draft1 v2	08/01/2017	RSAW Task Force	Modified Question to clarify applicability
Draft1 v3	08/02/2017	RSAW Task Force	Response to MRO comments. Moved Questions 1 and 2 above R1. Made text changes to Q1 and to R2 Compliance Assessment Approach.
Draft1 v4	08/07/2017	RSAW Task Force, 2016-02 SDT	Response to TexasRE and SDT comments. Clarified scope of Q1 to be data transmitted between Control Centers. Removed extra space from Auditor Notes.
Draft2 v1	10/27/2017	RSAW Task Force	Modified title. Modified Q2 to conform with new language. Modified R1 with new Requirement text and new Compliance Assessment Approach. Modified R2 with new Compliance Assessment Approach. Removed Operational Planning Analysis from the Selected Glossary Terms. Modified footer with revised version and date.
Draft2 v2	11/27/2017	RSAW Task Force, Standard Drafting Team	Response to comments: • RF: Footnote 1 page 1 added space after “references.” • RF: Changed “Tasf” to “Task” in Revision History. • Response to SERC CIPC and Southern Company comments to Draft 1. • Modified Question 1 to include reference to CIP-002. • Added an item to the R1 Compliance Assessment Approach to verify the effectiveness of the process. • Modified the R2 Compliance Assessment Approaches to clarify that the review is for implementation.
Draft3 v0	03/20/2018	RSAW Task Force	Modified for Draft 3 language: • Removed Requirement R2 • Modified Requirement R1 language to match the Standard • Modified the R1 Compliannce Assessment Approach

			• Removed "CIP Exceptional Circumstance" from the Selected Glossary Terms • Revised the definition of "Control Center" in Selected Glossary Terms to match the definition posted alongside CIP-012-1 Draft 3
Draft3 v1	04/03/2018	ERO Enterprise	• Consideration of Comments from RF o Changed Sampling Methodology section to match current NERC documents. Will also need to be reflected in the RSAW Template.
Draft3 v2	4/25/2018	NERC Legal	Addressed comments. No text changes were made.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Reliability Standard Audit Worksheet[1]

CIP-012-1 – Cyber Security – Communications between Control Centers

This section to be completed by the Compliance Enforcement Authority.

Audit ID:	Audit ID if available; or REG-NCRnnnnn-YYYYMMDD
Registered Entity:	Registered name of entity being audited
NCR Number:	NCRnnnnn
Compliance Enforcement Authority:	Region or NERC performing audit
Compliance Assessment Date(s)[2]:	Month DD, YYYY, to Month DD, YYYY
Compliance Monitoring Method:	[On-site Audit | Off-site Audit | Spot Check]
Names of Auditors:	Supplied by CEA

Applicability of Requirements

	BA	DP	GO	GOP	PA/PC	RC	RP	RSG	TO	TOP	TP	TSP
R1	X		X	X		X			X	X		
~~**R2**~~	~~X~~		~~X~~	~~X~~		~~X~~			~~X~~	~~X~~		

Legend:

Text with blue background:	Fixed text – do not edit
Text entry area with Green background:	Entity-supplied information
Text entry area with white background:	Auditor-supplied information

[1] NERC developed this Reliability Standard Audit Worksheet (RSAW) language in order to facilitate NERC's and the Regional Entities' assessment of a registered entity's compliance with this Reliability Standard. The NERC RSAW language is written to specific versions of each NERC Reliability Standard. Entities using this RSAW should choose the version of the RSAW applicable to the Reliability Standard being assessed. While the information included in this RSAW provides some of the methodology that NERC has elected to use to assess compliance with the requirements of the Reliability Standard, this document should not be treated as a substitute for the Reliability Standard or viewed as additional Reliability Standard requirements. In all cases, the Regional Entity should rely on the language contained in the Reliability Standard itself, and not on the language contained in this RSAW, to determine compliance with the Reliability Standard. NERC's Reliability Standards can be found on NERC's website. Additionally, NERC Reliability Standards are updated frequently, and this RSAW may not necessarily be updated with the same frequency. Therefore, it is imperative that entities treat this RSAW as a reference document only, and not as a substitute or replacement for the Reliability Standard. It is the responsibility of the registered entity to verify its compliance with the latest approved version of the Reliability Standards, by the applicable governmental authority, relevant to its registration status.

The RSAW may provide a non-exclusive list, for informational purposes only, of examples of the types of evidence a registered entity may produce or may be asked to produce to demonstrate compliance with the Reliability Standard. A registered entity's adherence to the examples contained within this RSAW does not necessarily constitute compliance with the applicable Reliability Standard, and NERC and the Regional Entity using this RSAW reserve the right to request additional evidence from the registered entity that is not included in this RSAW. This RSAW may include excerpts from FERC Orders and other regulatory references which are provided for ease of reference only, and this document does not necessarily include all applicable Order provisions. In the event of a discrepancy between FERC Orders, and the language included in this document, FERC Orders shall prevail.

[2] Compliance Assessment Date(s): The date(s) the actual compliance assessment (on-site audit, off-site spot check, etc.) occurs.

Findings

(This section to be completed by the Compliance Enforcement Authority)

Req.	Finding	Summary and Documentation	Functions Monitored
R1			
~~R2~~			

Req.	Areas of Concern

Req.	Recommendations

Req.	Positive Observations

Subject Matter Experts

Identify the Subject Matter Expert(s) responsible for this Reliability Standard.

Registered Entity Response (Required; Insert additional rows if needed):

SME Name	Title	Organization	Requirement(s)

Registered Entity Response (Required):

Question 1: Does the Registered Entity own or operate a Control Center? ☐ Yes ☐ No

If no:

1. Provide evidence in the space that the Registered Entity does not own or operate one or more Control Centers. This evidence may include, but is not limited to:
   - Evidence that the Registered Entity does not own or operate a Control Center; or
   - Evidence or a reference to evidence from the Registered Entity's CIP-002 compliance program that demonstrates the entity does not own or operate a Control Center.[A1][A2]
2. The remainder of this RSAW may be left blank.

[Note: A separate spreadsheet or other document may be used. If so, provide the document reference below.]

R1 Supporting Evidence and Documentation

R1. The Responsible Entity shall ~~develop~~ implement one or more documented plan(s) to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring ~~and control~~ data while being transmitted between any Control Centers. This requirement excludes oral communications. The plan shall include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1 Identification of security protection used to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring ~~and control~~ data while being transmitted between Control Centers;

1.2 Identification of ~~demarcation point(s)~~ where the Responsible Entity applied security protection ~~is applied~~ for transmitting Real-time Assessment and Real-time monitoring ~~and control~~ data between Control Centers; and

1.3 If ~~Identification of roles and responsibilities of each Responsible Entity for applying security protection to the transmission of Real-time Assessment and Real-time monitoring and control data between Control Centers, when~~ the Control Centers are owned or operated by different Responsible Entities, identify the responsibilities of each Responsible Entity for applying security protection to the transmission of Real-time Assessment and Real-time monitoring data between those Control Centers.

M1. Evidence may include, but is not limited to, documented plan(s) that meet the security objective of Requirement R1 and documentation demonstrating the implementation of the plan(s).

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-012-1, R1

This section to be completed by the Compliance Enforcement Authority

	If the Registered Entity has answered "No" to Question 1, verify the Registered Entity does not own or operate a Control Center. Note: If the Registered Entity does not own or operate a Control Center, the remainder of this RSAW is not applicable.
	Verify the entity has ~~developed~~ implemented one or more documented plan(s) to mitigate the risk of the unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring ~~and control~~ data while being transmitted between Control Centers.
	Verify the documented plans collectively include identification of security protection used to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring ~~and control~~ data while being transmitted between Control Centers.
	Verify the documented plans collectively include identification of ~~demarcation point(s)~~ where the Responsible Entity applied security protection ~~is applied~~ for transmitting Real-time Assessment and Real-time monitoring ~~and control~~ data between Control Centers.
	Verify the documented plans collectively include identification of ~~roles and~~ responsibilities of each Responsible Entity for applying security protection to the transmission of Real-time Assessment and Real-time monitoring ~~and control~~ data between Control Centers, when the Control Centers are owned or operated by different Responsible Entities.
	Verify the documented plans collectively achieve the security objective of mitigating the risk of the unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring ~~and control~~ data while being transmitted between Control Centers.[A3][A4]
Note to Auditor: 1. Oral communications are not in scope for CIP-012-1.	

Auditor Notes:

R2 Supporting Evidence and Documentation

R2. The Responsible Entity shall implement the plan(s) specified in Requirement R1, except under CIP Exceptional Circumstances.

M2. Evidence may include, but is not limited to, documentation to demonstrate implementation of methods to mitigate the risk of the unauthorized disclosure or modification of data in Requirement R1.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-012-1, R2

This section to be completed by the Compliance Enforcement Authority

	Verify the entity has implemented one or more documented plan(s) to mitigate the risk of the unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring and control data while being transmitted between Control Centers.
	Verify the entity has implemented the identified security protection used to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring and control data while being transmitted between Control Centers.
	Verify the entity has implemented the identified security protection at the identified demarcation point(s) where security protection is applied for transmitting Real-time Assessment and Real-time monitoring and control data between Control Centers; and
	If Control Centers are not owned and operated by the same Responsible Entity, verify the entity has identified roles and responsibilities of each Responsible Entity for applying security protection to the transmission of Real-time Assessment and Real-time monitoring and control data between Control Centers.
	If the Responsible Entity has declared and responded to CIP Exceptional Circumstances, verify the Responsible Entity has adhered to the applicable cyber security policies.
Note to Auditor: The Responsible Entity may reference a separate set of documents to demonstrate its response to any requirements impacted by CIP Exceptional Circumstances.	

Auditor Notes:

Additional Information:

Reliability Standard

The full text of CIP-012-1 may be found on the NERC Web Site (www.nerc.com) under "Program Areas & Departments", "Standards," "Reliability Standards."

In addition to the Reliability Standard, there is an applicable Implementation Plan available on the NERC Web Site.

In addition to the Reliability Standard, there is background information available on the NERC Web Site.

Capitalized terms in the Reliability Standard refer to terms in the NERC Glossary, which may be found on the NERC Web Site.

Sampling Methodology

Sampling is essential for auditing compliance with NERC Reliability Standards since it is not always possible or practical to test 100% of either the equipment, documentation, or both, associated with the full suite of enforceable standards. The Sampling Guide contained in the Compliance Monitoring and Enforcement Manual ~~Methodology Guidelines and Criteria~~ (see NERC website)~~, or sample guidelines,~~ provided by the Electric Reliability Organization help to establish a minimum sample set for monitoring and enforcement uses in audits of NERC Reliability Standards.

Regulatory Language

FERC Order 822 P53-56, 58, and 62

Selected Glossary Terms

The following Glossary terms are provided for convenience only. Please refer to the NERC web site for the current enforceable terms.

~~CIP Exceptional Circumstance~~
~~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.~~

Control Center
~~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, of: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for transmission Facilities at two or more locations, or 4) a Generator Operator for generation Facilities at two or more locations.~~
One or more facilities, including their associated data centers, that monitor and control the Bulk Electric System (BES) and also host operating personnel who:

1) perform the Real-time reliability-related tasks of a Reliability Coordinator; or

2) perform the Real-time reliability-related tasks of a Balancing Authority; or
3) perform the Real-time reliability-related tasks of a Transmission Operator for Transmission Facilities at two or more locations; or
4) can act independently as the Generator Operator to develop specific dispatch instructions for generation Facilities at two or more locations; or
5) can operate or direct the operation of a Transmission Owner's BES Transmission Facilities in Real-time.

Operating personnel do not include:
1) plant operators located at a generator plant site or personnel at a centrally located dispatch center who relay dispatch instructions without making any modifications; or
~~1)~~ Transmission Owner or Transmission Operator field switching personnel.
2)

Real-time Assessment
An evaluation of system conditions using Real-time data to assess existing (pre-Contingency) and potential (post-Contingency) operating conditions. The assessment shall reflect applicable inputs including, but not limited to: load, generation output levels, known Protection System and Special Protection System status or degradation, Transmission outages, generator outages, Interchange, Facility Ratings, and identified phase angle and equipment limitations. (Real-time Assessment may be provided through internal systems or through third-party services.)

Real-time
Present time as opposed to future time.

Revision History for RSAW

Version	Date	Reviewers	Revision Description
Draft1 v1	07/28/2017	NERC Stds Group	New document
Draft1 v2	08/01/2017	RSAW Task Force	Modified Question to clarify applicability
Draft1 v3	08/02/2017	RSAW Task Force	Response to MRO comments. Moved Questions 1 and 2 above R1. Made text changes to Q1 and to R2 Compliance Assessment Approach.
Draft1 v4	08/07/2017	RSAW Task Force, 2016-02 SDT	Response to TexasRE and SDT comments. Clarified scope of Q1 to be data transmitted between Control Centers. Removed extra space from Auditor Notes.
Draft2 v1	10/27/2017	RSAW Task Force	Modified title. Modified Q2 to conform with new language. Modified R1 with new Requirement text and new Compliance Assessment Approach. Modified R2 with new Compliance Assessment Approach. Removed Operational Planning Analysis from the Selected Glossary Terms. Modified footer with revised version and date.
Draft2 v2	11/27/2017	RSAW Task Force, Standard Drafting Team	Response to comments: • RF: Footnote 1 page 1 added space after "references." • RF: Changed "Tasf" to "Task" in Revision History. • Response to SERC CIPC and Southern Company comments to Draft 1. • Modified Question 1 to include reference to CIP-002. • Added an item to the R1 Compliance Assessment Approach to verify the effectiveness of the process. • Modified the R2 Compliance Assessment Approaches to clarify that the review is for implementation.
Draft3 v0	03/20/2018	RSAW Task Force	Modified for Draft 3 language: • Removed Requirement R2 • Modified Requirement R1 language to match the Standard • Modified the R1 Complian~~a~~ince Assessment Approach

			• Removed "CIP Exceptional Circumstance" from the Selected Glossary Terms • Revised the definition of "Control Center" in Selected Glossary Terms to match the definition posted alongside CIP-012-1 Draft 3
Draft3 v1	04/03/2018	ERO Enterprise	• Consideration of Comments from RF o Changed Sampling Methodology section to match current NERC documents. Will also need to be reflected in the RSAW Template.
Draft3 v2	4/25/2018	NERC Legal	Addressed comments. No text changes were made.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Reminder

Project 2016-02 Modifications to CIP Standards

Initial and Additional Ballots and Non-binding Polls Open through April 30, 2018

Now Available

Initial ballots for the **Control Center Definition** and its **Implementation Plan**, additional ballots for **CIP-002-6** and **CIP-012-1** and the associated non-binding polls of the associated Violation Risk Factors and Violation Severity Levels are open through **8 p.m. Eastern, Monday, April 30, 2018.**

The standard drafting team's considerations of the responses received from the last comment period for **CIP-002-6** and **CIP-012-1** are reflected in these drafts of the standards.

Balloting

Members of the ballot pools associated with this project can log in and submit their votes by accessing the Standards Balloting and Commenting System (SBS) here. If you experience any difficulties navigating the SBS, contact Wendy Muller.

- *If you are having difficulty accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out, contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern).*
- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*
- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Note: If a member cast a vote in the previous ballot, that vote will not carry over to the additional ballot. It is the responsibility of the registered voter in the ballot pool to cast a vote again in the additional ballot. To ensure a quorum is reached, if you do not want to vote affirmative or negative, cast an abstention.

Next Steps

The ballot results will be announced and posted on the project page. The drafting team will review all responses received during the comment period and determine the next steps of the project.

For information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact Mat Bunch at (404) 446-9785 or Jordan Mallory at (404) 446-2589.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2016-02 Modifications to CIP Standards

Formal Comment Periods Open through April 30, 2018
Ballot Pools Forming through April 16, 2018

Now Available

Three formal comment periods are open through **8 p.m. Eastern, Monday, April 30, 2018** for:

1. **CIP-002-6 – Cyber Security - BES Cyber System Categorization**
2. **CIP-012-1 – Cyber Security - Communications between Control Centers**
3. **Project 2016-02 Modifications to NERC Glossary of Terms Used in Reliability Standards – Control Center**

Commenting

Use the Standards Balloting and Commenting System (SBS) to submit comments. If you experience difficulties navigating the SBS, contact Wendy Muller. Unofficial Word versions of the comment forms are posted on the project page.

Ballot Pools

Ballot pools are being formed through **8 p.m. Eastern, Monday, April 16, 2018** for the **Control Center Definition** and its **Implementation Plan**. Registered Ballot Body members can join the ballot pools here.

- *If you are having difficulty accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out, contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern).*
- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*
- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Next Steps

The initial ballots for the **Control Center Definition** and its **Implementation Plan** will be conducted **April 20-30, 2018**. Additional ballots for **CIP-002-6** and **CIP-012-1** and the associated non-binding polls of the associated Violation Risk Factors and Violation Severity Levels will be conducted **April 20-30, 2018.**

For information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact Mat Bunch at (404) 446-9785 or Jordan Mallory at (404) 446-2589.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/130)
Ballot Name: 2016-02 Modifications to CIP Standards CIP-012-1 AB 3 ST
Voting Start Date: 4/20/2018 12:01:00 AM
Voting End Date: 4/30/2018 8:00:00 PM
Ballot Type: ST
Ballot Activity: AB
Ballot Series: 3
Total # Votes: 242
Total Ballot Pool: 309
Quorum: 78.32
Weighted Segment Value: 83.71

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	80	1	48	0.828	10	0.172	0	5	17
Segment: 2	7	0.6	5	0.5	1	0.1	0	0	1
Segment: 3	73	1	47	0.887	6	0.113	0	5	15
Segment: 4	17	1	12	0.857	2	0.143	0	1	2
Segment: 5	73	1	37	0.771	11	0.229	0	2	23
Segment: 6	46	1	27	0.75	9	0.25	0	2	8
Segment: 7	2	0.1	1	0.1	0	0	0	0	1
Segment: 8	3	0.3	3	0.3	0	0	0	0	0
Segment: 9	1	0.1	1	0.1	0	0	0	0	0
Segment: 10	7	0.7	6	0.6	1	0.1	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Totals:	309	6.8	187	5.692	40	1.108	0	15	67

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Affirmative	N/A
1	Allete - Minnesota Power, Inc.	Jamie Monette		Abstain	N/A
1	American Transmission Company, LLC	Douglas Johnson		Affirmative	N/A
1	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	John Shaver		Negative	Third-Party Comments
1	Associated Electric Cooperative, Inc.	Ryan Ziegler		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Joe Tarantino	Affirmative	N/A
1	Basin Electric Power Cooperative	David Rudolph		None	N/A
1	BC Hydro and Power Authority	Patricia Robertson		Affirmative	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Bonneville Power Administration	Kammy Rogers-Holliday		Affirmative	N/A
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		None	N/A
1	Cedar Falls Utilities	Adam Peterson		None	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Hudson Gas & Electric Corp.	Frank Pace		Negative	Third-Party Comments
1	City Utilities of Springfield, Missouri	Michael Buyce		Affirmative	N/A
1	CMS Energy - Consumers Energy Company	James Anderson		Negative	Comments Submitted
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Larry Nash		Negative	Comments Submitted
1	Duke Energy	Laura Lee		Negative	Comments Submitted
1	Edison International - Southern California Edison Company	Steven Mavis		Affirmative	N/A
1	Entergy - Entergy Services, Inc.	Oliver Burke		Negative	Comments Submitted
1	Eversource Energy	Quintin Lee		Affirmative	N/A
1	Exelon	Chris Scanlon		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	Karen Yoder		Affirmative	N/A
1	Great Plains Energy - Kansas City Power and Light Co.	James McBee	Douglas Webb	Affirmative	N/A
1	Great River Energy	Gordon Pietsch		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Affirmative	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Affirmative	N/A
1	IDACORP - Idaho Power Company	Laura Nelson		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz		None	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Stephanie Burns	Abstain	N/A
1	Lincoln Electric System	Danny Pudenz		Affirmative	N/A
1	Long Island Power Authority	Robert Ganley		None	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		Affirmative	N/A
1	Lower Colorado River Authority	Michael Shaw		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		None	N/A
1	Manitoba Hydro	Mike Smith		Affirmative	N/A
1	MEAG Power	David Weekley	Scott Miller	Abstain	N/A
1	Memphis Light, Gas and Water Division	Allan Long		None	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A
1	Muscatine Power and Water	Andy Kurriger		Affirmative	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Affirmative	N/A
1	Nebraska Public Power District	Jamison Cawley		Affirmative	N/A
1	New York Power Authority	Salvatore Spagnolo		Affirmative	N/A
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Affirmative	N/A
1	Northeast Missouri Electric Power Cooperative	Kevin White		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Ohio Valley Electric Corporation	Scott Cunningham		Affirmative	N/A
1	Omaha Public Power District	Doug Peterchuck		None	N/A
1	Oncor Electric Delivery	Lee Maurer	Tho Tran	Affirmative	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		Affirmative	N/A
1	Peak Reliability	Scott Downey		None	N/A
1	PNM Resources - Public Service Company of New Mexico	Laurie Williams		None	N/A
1	PPL Electric Utilities Corporation	Brenda Truhe		Affirmative	N/A
1	PSEG - Public Service Electric and Gas Co.	Joseph Smith		Affirmative	N/A
1	Public Utility District No. 1 of Chelan County	Jeff Kimbell		Abstain	N/A
1	Public Utility District No. 1 of Snohomish County	Long Duong		Affirmative	N/A
1	Puget Sound Energy, Inc.	Theresa Rakowsky		None	N/A
1	Sacramento Municipal Utility District	Arthur Starkovich	Joe Tarantino	Affirmative	N/A
1	Salt River Project	Steven Cobb		None	N/A
1	Santee Cooper	Chris Wagner		None	N/A
1	SCANA - South Carolina Electric and Gas Co.	Tom Hanzlik		None	N/A
1	Seattle City Light	Pawel Krupa		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Seminole Electric Cooperative, Inc.	Mark Churilla		Abstain	N/A
1	Sempra - San Diego Gas and Electric	Mo Derbas	Jeff Johnson	None	N/A
1	Sho-Me Power Electric Cooperative	Peter Dawson		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Katherine Prewitt		Affirmative	N/A
1	Southern Indiana Gas and Electric Co.	Steve Rawlinson		Affirmative	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell		Negative	Comments Submitted
1	Tennessee Valley Authority	Howell Scott		Affirmative	N/A
1	Tri-State G and T Association, Inc.	Tracy Sliman		Negative	Comments Submitted
1	U.S. Bureau of Reclamation	Richard Jackson		Negative	Comments Submitted
1	Westar Energy	Kevin Giles		Affirmative	N/A
1	Western Area Power Administration	sean erickson		Affirmative	N/A
1	Xcel Energy, Inc.	Dean Schiro		Affirmative	N/A
2	California ISO	Richard Vine		Affirmative	N/A
2	Electric Reliability Council of Texas, Inc.	Brandon Gleason		Affirmative	N/A
2	Independent Electricity System Operator	Leonard Kula		Affirmative	N/A
2	ISO New England, Inc.	Michael Puscas		None	N/A
2	Midcontinent ISO, Inc.	Ellen Oswald		Negative	Comments Submitted
2	New York Independent System Operator	Gregory Campoli		Affirmative	N/A
2	PJM Interconnection, L.L.C.	Mark Holman		Affirmative	N/A
3	AEP	Aaron Austin		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	AES - Indianapolis Power and Light Co.	Bette White		Affirmative	N/A
3	APS - Arizona Public Service Co.	Vivian Vo		Affirmative	N/A
3	Arkansas Electric Cooperative Corporation	Philip Huff		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	W. Dwayne Preston		Affirmative	N/A
3	Basin Electric Power Cooperative	Jeremy Voll		Affirmative	N/A
3	BC Hydro and Power Authority	Hootan Jarollahi		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Annette Johnston	Darnez Gresham	Negative	Comments Submitted
3	Bonneville Power Administration	Rebecca Berdahl		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City of Farmington	Linda Jacobson-Quinn		Abstain	N/A
3	City of Leesburg	Chris Adkins		None	N/A
3	City of Vero Beach	Ginny Beigel	Brandon McCormick	Negative	Comments Submitted
3	City Utilities of Springfield, Missouri	Scott Williams		Affirmative	N/A
3	Cleco Corporation	Michelle Corley	Louis Guidry	Affirmative	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
3	Cowlitz County PUD	Russell Noble		Negative	Comments Submitted
3	Duke Energy	Lee Schuster		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Edison International - Southern California Edison Company	Romel Aquino		None	N/A
3	Empire District Electric Co.	Kalem Long		None	N/A
3	Eversource Energy	Mark Kenny		Affirmative	N/A
3	Exelon	John Bee		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great Plains Energy - Kansas City Power and Light Co.	Jessica Tucker	Douglas Webb	Affirmative	N/A
3	Great River Energy	Brian Glover		Affirmative	N/A
3	Hydro One Networks, Inc.	Paul Malozewski		Affirmative	N/A
3	KAMO Electric Cooperative	Ted Hilmes		None	N/A
3	Lincoln Electric System	Jason Fortik		Affirmative	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	Manitoba Hydro	Karim Abdel-Hadi		Affirmative	N/A
3	MEAG Power	Roger Brand	Scott Miller	Abstain	N/A
3	Modesto Irrigation District	Jack Savage	Nick Braden	None	N/A
3	Muscatine Power and Water	Seth Shoemaker		Affirmative	N/A
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A
3	New York Power Authority	David Rivera		Affirmative	N/A
3	NiSource - Northern Indiana Public Service Co.	Aimee Harris		Affirmative	N/A
3	North Carolina Electric Membership Corporation	doug white	Scott Brame	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Affirmative	N/A
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen		None	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	OTP - Otter Tail Power Company	Wendi Olson		Affirmative	N/A
3	Owensboro Municipal Utilities	Thomas Lyons		None	N/A
3	Platte River Power Authority	Jeff Landis		Abstain	N/A
3	PNM Resources - Public Service Company of New Mexico	Lynn Goldstein		Affirmative	N/A
3	Portland General Electric Co.	Angela Gaines		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	Charles Freibert		Affirmative	N/A
3	PSEG - Public Service Electric and Gas Co.	Jeffrey Mueller		Affirmative	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Abstain	N/A
3	Puget Sound Energy, Inc.	Tim Womack		None	N/A
3	Rutherford EMC	Tom Haire		None	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Joe Tarantino	Affirmative	N/A
3	Salt River Project	Robert Kondziolka		Negative	Comments Submitted
3	Santee Cooper	James Poston		None	N/A
3	SCANA - South Carolina Electric and Gas Co.	Scott Parker		None	N/A
3	Seattle City Light	Tuan Tran		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Seminole Electric Cooperative, Inc.	James Frauen		Abstain	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia	Harold Sherrill	Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jeff Neas		Affirmative	N/A
3	Silicon Valley Power - City of Santa Clara	Val Ridad		None	N/A
3	Snohomish County PUD No. 1	Mark Oens		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Fred Frederick		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson		Negative	Comments Submitted
3	TECO - Tampa Electric Co.	Ronald Donahey		None	N/A
3	Tennessee Valley Authority	Ian Grant		None	N/A
3	Tri-State G and T Association, Inc.	Janelle Marriott Gill		None	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Affirmative	N/A
3	Westar Energy	Bo Jones		Affirmative	N/A
3	Xcel Energy, Inc.	Michael Ibold		Affirmative	N/A
4	American Public Power Association	Jack Cashin		None	N/A
4	Arkansas Electric Cooperative Corporation	Alice Wright		Affirmative	N/A
4	Austin Energy	Esther Weekes		Affirmative	N/A
4	City of Clewiston	Lynne Mila	Brandon McCormick	Negative	Comments Submitted
4	City Utilities of Springfield, Missouri	John Allen		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Aubrey Short		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Georgia System Operations Corporation	Guy Andrews		Affirmative	N/A
4	Indiana Municipal Power Agency	Jack Alvey	Scott Berry	Abstain	N/A
4	National Rural Electric Cooperative Association	Barry Lawson		Affirmative	N/A
4	North Carolina Electric Membership Corporation	John Lemire	Scott Brame	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John Martinsen		Affirmative	N/A
4	Sacramento Municipal Utility District	Beth Tincher	Joe Tarantino	Affirmative	N/A
4	Seattle City Light	Hao Li		Affirmative	N/A
4	Seminole Electric Cooperative, Inc.	Charles Wubbena		None	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho		Negative	Comments Submitted
4	Utility Services, Inc.	Brian Evans-Mongeon		Affirmative	N/A
4	WEC Energy Group, Inc.	Anthony Jankowski		Affirmative	N/A
5	Acciona Energy North America	George Brown		Affirmative	N/A
5	AEP	Thomas Foltz		Affirmative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Affirmative	N/A
5	APS - Arizona Public Service Co.	Kelsi Rigby		Affirmative	N/A
5	Arkansas Electric Cooperative Corporation	Moses Harris		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Brad Haralson		None	N/A
5	Austin Energy	Shirley Mathew		None	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Basin Electric Power Cooperative	Mike Kraft		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		None	N/A
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		Affirmative	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	BP Wind Energy North America Inc.	Carla Holly		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Affirmative	N/A
5	Cleco Corporation	Stephanie Huffman	Louis Guidry	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Negative	Comments Submitted
5	Colorado Springs Utilities	Jeff Icke		Negative	Comments Submitted
5	Con Ed - Consolidated Edison Co. of New York	William Winters	Alyson Slanover	Affirmative	N/A
5	Dairyland Power Cooperative	Tommy Drea		None	N/A
5	Dominion - Dominion Resources, Inc.	Lou Oberski		Negative	Comments Submitted
5	Duke Energy	Dale Goodwine		Negative	Comments Submitted
5	Edison International - Southern California Edison Company	Selene Willis		None	N/A
5	EDP Renewables North America LLC	Heather Morgan		Negative	Comments Submitted
5	Entergy	Jamie Prater		Negative	Comments Submitted
5	Exelon	Ruth Miller		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	FirstEnergy - FirstEnergy Solutions	Robert Loy		Affirmative	N/A
5	Great Plains Energy - Kansas City Power and Light Co.	Harold Wyble	Douglas Webb	Affirmative	N/A
5	Great River Energy	Preston Walsh		Affirmative	N/A
5	Gridforce Energy Management, LLC	David Blackshear		None	N/A
5	Hydro-Qu?bec Production	Junji Yamaguchi		None	N/A
5	JEA	John Babik		None	N/A
5	Kissimmee Utility Authority	Mike Blough	Brandon McCormick	Negative	Comments Submitted
5	Lakeland Electric	Jim Howard		None	N/A
5	Lincoln Electric System	Kayleigh Wilkerson		Affirmative	N/A
5	Los Angeles Department of Water and Power	Donald Sievertson		Affirmative	N/A
5	Manitoba Hydro	Yuguang Xiao		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	David Gordon		Affirmative	N/A
5	MEAG Power	Steven Grego	Scott Miller	Abstain	N/A
5	Muscatine Power and Water	Neal Nelson		Affirmative	N/A
5	NB Power Corporation	Laura McLeod		None	N/A
5	Nebraska Public Power District	Don Schmit		Affirmative	N/A
5	New York Power Authority	Erick Barrios		Affirmative	N/A
5	NextEra Energy	Allen Schriver		None	N/A
5	NiSource - Northern Indiana Public Service Co.	Dmitriy Bazylyuk		Affirmative	N/A
5	North Carolina Electric Membership Corporation	Robert Beadle	Scott Brame	Affirmative	N/A
5	Northern California Power Agency	Marty Hostler		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	OGE Energy - Oklahoma Gas and Electric Co.	John Rhea		Affirmative	N/A
5	Omaha Public Power District	Mahmood Safi		Affirmative	N/A
5	Ontario Power Generation Inc.	David Ramkalawan		Affirmative	N/A
5	OTP - Otter Tail Power Company	Cathy Fogale		Affirmative	N/A
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	JULIE HOSTRANDER		Affirmative	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Affirmative	N/A
5	Public Utility District No. 1 of Chelan County	Haley Sousa		Abstain	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Puget Sound Energy, Inc.	Eleanor Ewry		None	N/A
5	Sacramento Municipal Utility District	Susan Oto	Joe Tarantino	Affirmative	N/A
5	Salt River Project	Kevin Nielsen		Negative	Comments Submitted
5	Santee Cooper	Tommy Curtis		None	N/A
5	SCANA - South Carolina Electric and Gas Co.	Alyssa Hubbard		None	N/A
5	Seattle City Light	Faz Kasraie		None	N/A
5	Seminole Electric Cooperative, Inc.	Brenda Atkins		None	N/A
5	Sempra - San Diego Gas and Electric	Daniel Frank	Andrey Komissarov	None	N/A
5	Silicon Valley Power - City of Santa Clara	Sandra Pacheco		None	N/A
5	Southern Company - Southern Company Generation	William D. Shultz		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	SunPower	Bradley Collard		None	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin		None	N/A
5	Talen Generation, LLC	Matthew McMillan		None	N/A
5	TECO - Tampa Electric Co.	Frank L Busot		None	N/A
5	Tennessee Valley Authority	M Lee Thomas		Affirmative	N/A
5	U.S. Bureau of Reclamation	Wendy Center		Negative	Comments Submitted
5	WEC Energy Group, Inc.	Linda Horn		Affirmative	N/A
5	Xcel Energy, Inc.	Gerry Huitt		Affirmative	N/A
6	APS - Arizona Public Service Co.	Jonathan Aragon		Affirmative	N/A
6	Arkansas Electric Cooperative Corporation	Bruce Walkup		Affirmative	N/A
6	Austin Energy	Andrew Gallo		Affirmative	N/A
6	Basin Electric Power Cooperative	Paul Huettl		Affirmative	N/A
6	Berkshire Hathaway - PacifiCorp	Sandra Shaffer		Negative	Comments Submitted
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
6	Cleco Corporation	Robert Hirchak	Louis Guidry	Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Robert Winston		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
6	Duke Energy	Greg Cecil		Negative	Comments Submitted
6	Edison International - Southern California Edison Company	Kenya Streeter		Affirmative	N/A
6	Entergy	Julie Hall		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Exelon	Becky Webb		Negative	Comments Submitted
6	FirstEnergy - FirstEnergy Solutions	Ann Ivanc		Affirmative	N/A
6	Florida Municipal Power Pool	Tom Reedy	Brandon McCormick	Negative	Comments Submitted
6	Great Plains Energy - Kansas City Power and Light Co.	Jim Flucke	Douglas Webb	Affirmative	N/A
6	Lincoln Electric System	Eric Ruskamp		Affirmative	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Affirmative	N/A
6	Luminant - Luminant Energy	Brenda Hampton		Affirmative	N/A
6	Manitoba Hydro	Blair Mukanik		None	N/A
6	Modesto Irrigation District	James McFall	Nick Braden	None	N/A
6	Muscatine Power and Water	Ryan Streck	Amie Shuger McConnaha	Affirmative	N/A
6	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joe O'Brien		Affirmative	N/A
6	Northern California Power Agency	Dennis Sismaet		Negative	Comments Submitted
6	OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay		Affirmative	N/A
6	Omaha Public Power District	Joel Robles		None	N/A
6	Portland General Electric Co.	Daniel Mason		Affirmative	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
6	Public Utility District No. 1 of Chelan County	Davis Jelusich		Abstain	N/A
6	Public Utility District No. 2 of Grant County, Washington	LeRoy Patterson		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Sacramento Municipal Utility District	Jamie Cutlip	Joe Tarantino	Affirmative	N/A
6	Salt River Project	Bobby Olsen		Negative	Comments Submitted
6	Santee Cooper	Michael Brown		None	N/A
6	Seattle City Light	Charles Freeman		Affirmative	N/A
6	Seminole Electric Cooperative, Inc.	Trudy Novak		Abstain	N/A
6	Snohomish County PUD No. 1	Franklin Lu		Affirmative	N/A
6	Southern Company - Southern Company Generation and Energy Marketing	Jennifer Sykes		Affirmative	N/A
6	Southern Indiana Gas and Electric Co.	Brad Lisembee		None	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Rick Applegate		Negative	Comments Submitted
6	Talen Energy Marketing, LLC	Jennifer Hohenshilt		None	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Affirmative	N/A
6	WEC Energy Group, Inc.	David Hathaway		Affirmative	N/A
6	Westar Energy	Megan Wagner		Affirmative	N/A
6	Xcel Energy, Inc.	Carrie Dixon		Affirmative	N/A
7	Exxon Mobil	Jay Barnett		None	N/A
7	Luminant Mining Company LLC	Stewart Rake		Affirmative	N/A
8	David Kiguel	David Kiguel		Affirmative	N/A
8	Massachusetts Attorney General	Frederick Plett		Affirmative	N/A
8	Roger Zaklukiewicz	Roger Zaklukiewicz		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson		Affirmative	N/A
10	Midwest Reliability Organization	Russel Mountjoy		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Affirmative	N/A
10	Northeast Power Coordinating Council	Guy V. Zito		Affirmative	N/A
10	ReliabilityFirst	Anthony Jablonski		Affirmative	N/A
10	SERC Reliability Corporation	Drew Slabaugh		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Negative	Comments Submitted
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 309 of 309 entries

BALLOT RESULTS

Ballot Name: 2016-02 Modifications to CIP Standards CIP-012-1 Non-binding Poll AB 3 NB
Voting Start Date: 4/20/2018 12:01:00 AM
Voting End Date: 4/30/2018 8:00:00 PM
Ballot Type: NB
Ballot Activity: AB
Ballot Series: 3
Total # Votes: 221
Total Ballot Pool: 290
Quorum: 76.21
Weighted Segment Value: 79.78

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 1	75	1	36	0.837	7	0.163	14	18
Segment: 2	7	0.5	4	0.4	1	0.1	1	1
Segment: 3	70	1	36	0.837	7	0.163	10	17
Segment: 4	14	1	8	0.8	2	0.2	2	2
Segment: 5	69	1	28	0.737	10	0.263	9	22
Segment: 6	42	1	20	0.714	8	0.286	6	8
Segment: 7	2	0.1	1	0.1	0	0	0	1
Segment: 8	3	0.3	3	0.3	0	0	0	0
Segment: 9	1	0.1	1	0.1	0	0	0	0
Segment: 10	7	0.6	5	0.5	1	0.1	1	0
Totals:	290	6.6	142	5.326	36	1.274	43	69

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Affirmative	N/A
1	American Transmission Company, LLC	Douglas Johnson		Affirmative	N/A
1	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	John Shaver		Negative	Comments Submitted
1	Associated Electric Cooperative, Inc.	Ryan Ziegler		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Joe Tarantino	Affirmative	N/A
1	Basin Electric Power Cooperative	David Rudolph		None	N/A
1	BC Hydro and Power Authority	Patricia Robertson		Abstain	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Negative	Comments Submitted
1	Bonneville Power Administration	Kammy Rogers-Holliday		Affirmative	N/A
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		None	N/A
1	Cedar Falls Utilities	Adam Peterson		None	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Hudson Gas & Electric Corp.	Frank Pace		Abstain	N/A
1	City Utilities of Springfield, Missouri	Michael Buyce		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Larry Nash		Abstain	N/A
1	Duke Energy	Laura Lee		Negative	Comments Submitted
1	Edison International - Southern California Edison Company	Steven Mavis		Affirmative	N/A
1	Entergy - Entergy Services, Inc.	Oliver Burke		Negative	Comments Submitted
1	Eversource Energy	Quintin Lee		Affirmative	N/A
1	Exelon	Chris Scanlon		Abstain	N/A
1	FirstEnergy - FirstEnergy Corporation	Karen Yoder		Affirmative	N/A
1	Great Plains Energy - Kansas City Power and Light Co.	James McBee	Douglas Webb	Affirmative	N/A
1	Great River Energy	Gordon Pietsch		None	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Affirmative	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Affirmative	N/A
1	IDACORP - Idaho Power Company	Laura Nelson		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz		None	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Stephanie Burns	Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Lincoln Electric System	Danny Pudenz		Affirmative	N/A
1	Long Island Power Authority	Robert Ganley		None	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	Michael Shaw		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		None	N/A
1	Manitoba Hydro	Mike Smith		Affirmative	N/A
1	MEAG Power	David Weekley	Scott Miller	Abstain	N/A
1	Memphis Light, Gas and Water Division	Allan Long		None	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A
1	Muscatine Power and Water	Andy Kurriger		Abstain	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Affirmative	N/A
1	Nebraska Public Power District	Jamison Cawley		Abstain	N/A
1	New York Power Authority	Salvatore Spagnolo		Affirmative	N/A
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Affirmative	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Affirmative	N/A
1	Northeast Missouri Electric Power Cooperative	Kevin White		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Ohio Valley Electric Corporation	Scott Cunningham		Affirmative	N/A
1	Omaha Public Power District	Doug Peterchuck		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	OTP - Otter Tail Power Company	Charles Wicklund		Affirmative	N/A
1	Peak Reliability	Scott Downey		None	N/A
1	PNM Resources - Public Service Company of New Mexico	Laurie Williams		Negative	Comments Submitted
1	PPL Electric Utilities Corporation	Brenda Truhe		Abstain	N/A
1	PSEG - Public Service Electric and Gas Co.	Joseph Smith		Abstain	N/A
1	Public Utility District No. 1 of Chelan County	Jeff Kimbell		None	N/A
1	Public Utility District No. 1 of Snohomish County	Long Duong		Affirmative	N/A
1	Puget Sound Energy, Inc.	Theresa Rakowsky		None	N/A
1	Sacramento Municipal Utility District	Arthur Starkovich	Joe Tarantino	Affirmative	N/A
1	Salt River Project	Steven Cobb		None	N/A
1	Santee Cooper	Chris Wagner		None	N/A
1	SCANA - South Carolina Electric and Gas Co.	Tom Hanzlik		None	N/A
1	Seattle City Light	Pawel Krupa		Affirmative	N/A
1	Seminole Electric Cooperative, Inc.	Mark Churilla		Abstain	N/A
1	Sempra - San Diego Gas and Electric	Mo Derbas	Jeff Johnson	None	N/A
1	Sho-Me Power Electric Cooperative	Peter Dawson		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Katherine Prewitt		Affirmative	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell		Negative	Comments Submitted
1	Tennessee Valley Authority	Howell Scott		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Tri-State G and T Association, Inc.	Tracy Sliman		Abstain	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Negative	Comments Submitted
1	Westar Energy	Kevin Giles		Affirmative	N/A
1	Western Area Power Administration	sean erickson		Abstain	N/A
2	California ISO	Richard Vine		Affirmative	N/A
2	Electric Reliability Council of Texas, Inc.	Brandon Gleason		Affirmative	N/A
2	Independent Electricity System Operator	Leonard Kula		Affirmative	N/A
2	ISO New England, Inc.	Michael Puscas		None	N/A
2	Midcontinent ISO, Inc.	Ellen Oswald		Negative	Comments Submitted
2	New York Independent System Operator	Gregory Campoli		Abstain	N/A
2	PJM Interconnection, L.L.C.	Mark Holman		Affirmative	N/A
3	AEP	Aaron Austin		Affirmative	N/A
3	AES - Indianapolis Power and Light Co.	Bette White		Affirmative	N/A
3	APS - Arizona Public Service Co.	Vivian Vo		Affirmative	N/A
3	Arkansas Electric Cooperative Corporation	Philip Huff		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	W. Dwayne Preston		Affirmative	N/A
3	Basin Electric Power Cooperative	Jeremy Voll		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Annette Johnston	Darnez Gresham	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Bonneville Power Administration	Rebecca Berdahl		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City of Farmington	Linda Jacobson-Quinn		Abstain	N/A
3	City of Leesburg	Chris Adkins		None	N/A
3	City of Vero Beach	Ginny Beigel	Brandon McCormick	Negative	Comments Submitted
3	City Utilities of Springfield, Missouri	Scott Williams		Affirmative	N/A
3	Cleco Corporation	Michelle Corley	Louis Guidry	Affirmative	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
3	Cowlitz County PUD	Russell Noble		Negative	Comments Submitted
3	Duke Energy	Lee Schuster		None	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		None	N/A
3	Eversource Energy	Mark Kenny		Affirmative	N/A
3	Exelon	John Bee		Abstain	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Negative	Comments Submitted
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great Plains Energy - Kansas City Power and Light Co.	Jessica Tucker	Douglas Webb	Affirmative	N/A
3	Great River Energy	Brian Glover		Affirmative	N/A
3	Hydro One Networks, Inc.	Paul Malozewski		Affirmative	N/A
3	KAMO Electric Cooperative	Ted Hilmes		None	N/A
3	Lincoln Electric System	Jason Fortik		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	Manitoba Hydro	Karim Abdel-Hadi		Affirmative	N/A
3	MEAG Power	Roger Brand	Scott Miller	Abstain	N/A
3	Modesto Irrigation District	Jack Savage	Nick Braden	None	N/A
3	Muscatine Power and Water	Seth Shoemaker		Affirmative	N/A
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Abstain	N/A
3	New York Power Authority	David Rivera		Affirmative	N/A
3	NiSource - Northern Indiana Public Service Co.	Aimee Harris		Negative	Comments Submitted
3	North Carolina Electric Membership Corporation	doug white	Scott Brame	Affirmative	N/A
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Affirmative	N/A
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen		None	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	OTP - Otter Tail Power Company	Wendi Olson		Affirmative	N/A
3	Owensboro Municipal Utilities	Thomas Lyons		None	N/A
3	Platte River Power Authority	Jeff Landis		Abstain	N/A
3	PNM Resources - Public Service Company of New Mexico	Lynn Goldstein		Negative	Comments Submitted
3	Portland General Electric Co.	Angela Gaines		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	Charles Freibert		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	PSEG - Public Service Electric and Gas Co.	Jeffrey Mueller		Abstain	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Abstain	N/A
3	Puget Sound Energy, Inc.	Tim Womack		None	N/A
3	Rutherford EMC	Tom Haire		None	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Joe Tarantino	Affirmative	N/A
3	Salt River Project	Robert Kondziolka		Negative	Comments Submitted
3	Santee Cooper	James Poston		None	N/A
3	SCANA - South Carolina Electric and Gas Co.	Scott Parker		None	N/A
3	Seattle City Light	Tuan Tran		None	N/A
3	Seminole Electric Cooperative, Inc.	James Frauen		Abstain	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia	Harold Sherrill	Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jeff Neas		Affirmative	N/A
3	Silicon Valley Power - City of Santa Clara	Val Ridad		None	N/A
3	Snohomish County PUD No. 1	Mark Oens		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson		Affirmative	N/A
3	TECO - Tampa Electric Co.	Ronald Donahey		None	N/A
3	Tennessee Valley Authority	Ian Grant		None	N/A
3	Tri-State G and T Association, Inc.	Janelle Marriott Gill		None	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Westar Energy	Bo Jones		Affirmative	N/A
3	Xcel Energy, Inc.	Michael Ibold		Abstain	N/A
4	American Public Power Association	Jack Cashin		None	N/A
4	Austin Energy	Esther Weekes		Affirmative	N/A
4	City of Clewiston	Lynne Mila	Brandon McCormick	Negative	Comments Submitted
4	City Utilities of Springfield, Missouri	John Allen		Affirmative	N/A
4	Georgia System Operations Corporation	Guy Andrews		Affirmative	N/A
4	Indiana Municipal Power Agency	Jack Alvey	Scott Berry	Abstain	N/A
4	North Carolina Electric Membership Corporation	John Lemire	Scott Brame	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John Martinsen		Affirmative	N/A
4	Sacramento Municipal Utility District	Beth Tincher	Joe Tarantino	Affirmative	N/A
4	Seattle City Light	Hao Li		Affirmative	N/A
4	Seminole Electric Cooperative, Inc.	Charles Wubbena		None	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho		Negative	Comments Submitted
4	Utility Services, Inc.	Brian Evans-Mongeon		Abstain	N/A
4	WEC Energy Group, Inc.	Anthony Jankowski		Affirmative	N/A
5	Acciona Energy North America	George Brown		Abstain	N/A
5	AEP	Thomas Foltz		Affirmative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Abstain	N/A
5	APS - Arizona Public Service Co.	Kelsi Rigby		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Associated Electric Cooperative, Inc.	Brad Haralson		None	N/A
5	Austin Energy	Shirley Mathew		None	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	Basin Electric Power Cooperative	Mike Kraft		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		None	N/A
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		Affirmative	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	BP Wind Energy North America Inc.	Carla Holly		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Affirmative	N/A
5	Cleco Corporation	Stephanie Huffman	Louis Guidry	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Negative	Comments Submitted
5	Colorado Springs Utilities	Jeff Icke		Negative	Comments Submitted
5	Con Ed - Consolidated Edison Co. of New York	William Winters	Alyson Slanover	Affirmative	N/A
5	Dairyland Power Cooperative	Tommy Drea		None	N/A
5	Dominion - Dominion Resources, Inc.	Lou Oberski		Negative	Comments Submitted
5	Duke Energy	Dale Goodwine		Negative	Comments Submitted
5	Edison International - Southern California Edison Company	Selene Willis		None	N/A
5	EDP Renewables North America LLC	Heather Morgan		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Entergy	Jamie Prater		Negative	Comments Submitted
5	Exelon	Ruth Miller		Abstain	N/A
5	FirstEnergy - FirstEnergy Solutions	Robert Loy		Affirmative	N/A
5	Great Plains Energy - Kansas City Power and Light Co.	Harold Wyble	Douglas Webb	Affirmative	N/A
5	Great River Energy	Preston Walsh		Affirmative	N/A
5	Hydro-Qu?bec Production	Junji Yamaguchi		None	N/A
5	JEA	John Babik		None	N/A
5	Kissimmee Utility Authority	Mike Blough	Brandon McCormick	Negative	Comments Submitted
5	Lakeland Electric	Jim Howard		None	N/A
5	Lincoln Electric System	Kayleigh Wilkerson		Abstain	N/A
5	Los Angeles Department of Water and Power	Donald Sievertson		Affirmative	N/A
5	Manitoba Hydro	Yuguang Xiao		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	David Gordon		Abstain	N/A
5	MEAG Power	Steven Grego	Scott Miller	Abstain	N/A
5	Muscatine Power and Water	Neal Nelson		None	N/A
5	NB Power Corporation	Laura McLeod		Abstain	N/A
5	Nebraska Public Power District	Don Schmit		Affirmative	N/A
5	New York Power Authority	Erick Barrios		Affirmative	N/A
5	NextEra Energy	Allen Schriver		None	N/A
5	NiSource - Northern Indiana Public Service Co.	Dmitriy Bazylyuk		Affirmative	N/A
5	Northern California Power Agency	Marty Hostler		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	OGE Energy - Oklahoma Gas and Electric Co.	John Rhea		Affirmative	N/A
5	Omaha Public Power District	Mahmood Safi		Affirmative	N/A
5	Ontario Power Generation Inc.	David Ramkalawan		Affirmative	N/A
5	OTP - Otter Tail Power Company	Cathy Fogale		Affirmative	N/A
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	JULIE HOSTRANDER		None	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A
5	Public Utility District No. 1 of Chelan County	Haley Sousa		Abstain	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Puget Sound Energy, Inc.	Eleanor Ewry		None	N/A
5	Sacramento Municipal Utility District	Susan Oto	Joe Tarantino	Affirmative	N/A
5	Salt River Project	Kevin Nielsen		Negative	Comments Submitted
5	Santee Cooper	Tommy Curtis		None	N/A
5	SCANA - South Carolina Electric and Gas Co.	Alyssa Hubbard		None	N/A
5	Seattle City Light	Faz Kasraie		None	N/A
5	Seminole Electric Cooperative, Inc.	Brenda Atkins		None	N/A
5	Sempra - San Diego Gas and Electric	Jerome Gobby	Andrey Komissarov	Affirmative	N/A
5	Silicon Valley Power - City of Santa Clara	Sandra Pacheco		None	N/A
5	Southern Company - Southern Company Generation	William D. Shultz		Affirmative	N/A
5	SunPower	Bradley Collard		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin		None	N/A
5	Talen Generation, LLC	Matthew McMillan		Affirmative	N/A
5	TECO - Tampa Electric Co.	Frank L Busot		None	N/A
5	Tennessee Valley Authority	M Lee Thomas		None	N/A
5	U.S. Bureau of Reclamation	Wendy Center		Negative	Comments Submitted
5	Westar Energy	Laura Cox		Affirmative	N/A
6	APS - Arizona Public Service Co.	Jonathan Aragon		Affirmative	N/A
6	Arkansas Electric Cooperative Corporation	Bruce Walkup		Affirmative	N/A
6	Austin Energy	Andrew Gallo		Affirmative	N/A
6	Basin Electric Power Cooperative	Paul Huettl		Affirmative	N/A
6	Berkshire Hathaway - PacifiCorp	Sandra Shaffer		Negative	Comments Submitted
6	Cleco Corporation	Robert Hirchak	Louis Guidry	Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Robert Winston		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
6	Duke Energy	Greg Cecil		Negative	Comments Submitted
6	Edison International - Southern California Edison Company	Kenya Streeter		Affirmative	N/A
6	Entergy	Julie Hall		Negative	Comments Submitted
6	Exelon	Becky Webb		Abstain	N/A
6	FirstEnergy - FirstEnergy Solutions	Ann Ivanc		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Florida Municipal Power Pool	Tom Reedy	Brandon McCormick	Negative	Comments Submitted
6	Great Plains Energy - Kansas City Power and Light Co.	Jim Flucke	Douglas Webb	Affirmative	N/A
6	Lincoln Electric System	Eric Ruskamp		Abstain	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Affirmative	N/A
6	Luminant - Luminant Energy	Brenda Hampton		Affirmative	N/A
6	Manitoba Hydro	Blair Mukanik		None	N/A
6	Muscatine Power and Water	Ryan Streck	Amie Shuger McConnaha	Affirmative	N/A
6	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Abstain	N/A
6	NiSource - Northern Indiana Public Service Co.	Joe O'Brien		Affirmative	N/A
6	Northern California Power Agency	Dennis Sismaet		Negative	Comments Submitted
6	OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay		Affirmative	N/A
6	Omaha Public Power District	Joel Robles		None	N/A
6	Portland General Electric Co.	Daniel Mason		Affirmative	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		None	N/A
6	Public Utility District No. 1 of Chelan County	Davis Jelusich		Abstain	N/A
6	Public Utility District No. 2 of Grant County, Washington	LeRoy Patterson		None	N/A
6	Sacramento Municipal Utility District	Jamie Cutlip	Joe Tarantino	Affirmative	N/A
6	Salt River Project	Bobby Olsen		Negative	Comments Submitted
6	Santee Cooper	Michael Brown		None	N/A
6	Seattle City Light	Charles Freeman		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Seminole Electric Cooperative, Inc.	Trudy Novak		Abstain	N/A
6	Snohomish County PUD No. 1	Franklin Lu		Affirmative	N/A
6	Southern Company - Southern Company Generation and Energy Marketing	Jennifer Sykes		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Rick Applegate		Negative	Comments Submitted
6	Talen Energy Marketing, LLC	Jennifer Hohenshilt		Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Abstain	N/A
6	WEC Energy Group, Inc.	David Hathaway		None	N/A
6	Westar Energy	Megan Wagner		Affirmative	N/A
7	Exxon Mobil	Jay Barnett		None	N/A
7	Luminant Mining Company LLC	Stewart Rake		Affirmative	N/A
8	David Kiguel	David Kiguel		Affirmative	N/A
8	Massachusetts Attorney General	Frederick Plett		Affirmative	N/A
8	Roger Zaklukiewicz	Roger Zaklukiewicz		Affirmative	N/A
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson		Affirmative	N/A
10	Midwest Reliability Organization	Russel Mountjoy		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Affirmative	N/A
10	Northeast Power Coordinating Council	Guy V. Zito		Affirmative	N/A
10	ReliabilityFirst	Anthony Jablonski		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	SERC Reliability Corporation	Drew Slabaugh		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Negative	Comments Submitted
10	Western Electricity Coordinating Council	Steven Rueckert		Abstain	N/A

Previous 1 Next

Showing 1 to 290 of 290 entries

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2016-02 Modifications to CIP Standards

Formal Comment Periods Open through April 30, 2018
Ballot Pools Forming through April 16, 2018

Now Available

Three formal comment periods are open through **8 p.m. Eastern, Monday, April 30, 2018** for:

1. **CIP-002-6 – Cyber Security - BES Cyber System Categorization**
2. **CIP-012-1 – Cyber Security - Communications between Control Centers**
3. **Project 2016-02 Modifications to NERC Glossary of Terms Used in Reliability Standards – Control Center**

Commenting

Use the Standards Balloting and Commenting System (SBS) to submit comments. If you experience difficulties navigating the SBS, contact Wendy Muller. Unofficial Word versions of the comment forms are posted on the project page.

Ballot Pools

Ballot pools are being formed through **8 p.m. Eastern, Monday, April 16, 2018** for the **Control Center Definition** and its **Implementation Plan**. Registered Ballot Body members can join the ballot pools here.

- *If you are having difficulty accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out, contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern).*
- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*
- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Next Steps

The initial ballots for the **Control Center Definition** and its **Implementation Plan** will be conducted **April 20-30, 2018**. Additional ballots for **CIP-002-6** and **CIP-012-1** and the associated non-binding polls of the associated Violation Risk Factors and Violation Severity Levels will be conducted **April 20-30, 2018.**

For information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact Mat Bunch at (404) 446-9785 or Jordan Mallory at (404) 446-2589.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Comment Report

Project Name:	2016-02 Modifications to CIP Standards | CIP-012-1 Draft 3
Comment Period Start Date:	3/16/2018
Comment Period End Date:	4/30/2018
Associated Ballots:	2016-02 Modifications to CIP Standards CIP-012-1 AB 3 ST

There were 58 sets of responses, including comments from approximately 155 different people from approximately 108 companies representing 10 of the Industry Segments as shown in the table on the following pages.

Questions

1. Requirement R1: The SDT drafted CIP-012-1 Requirement R1 for the Responsible Entity to implement one or more documented plan(s) to mitigate the risk of the unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring data while being transmitted between any Control Centers. Do you agree with this revision? If not, please provide the basis for your disagreement and an alternate proposal.

2. Implementation Plan: The SDT established the Implementation Plan to make the standard effective the first day of the first calendar quarter that is twenty-four (24) calendar months after the effective date of the applicable governmental authority's order approving the standard, or as otherwise provided for by the applicable governmental authority. Do you agree with this proposal? If you think an alternate implementation time period is needed, please provide a detailed explanation of actions and time needed to meet the implementation deadline.

3. The SDT modified the draft Technical Rationale and Justification for CIP-012 to assist in understanding the technology and technical requirements in the Reliability Standard. It also contains information on the SDT's intent in drafting the requirements. Do you agree with the technology and technical requirements in the draft Technical Rationale and Justification? If you do not agree, or if you agree but have comments or suggestions for the draft Technical Rationale and Justification, please provide your recommendation and explanation.

4. The SDT modified the draft Implementation Guidance for CIP-012 to provide examples of how a Responsible Entity could comply with the requirements. The draft Implementation Guidance does not prescribe the only approach to compliance. Rather, it describes what the SDT believes would be effective ways to comply with the standard. See NERC's Compliance Guidance policy for information on Implementation Guidance. Do you agree with the draft Implementation Guidance? If you do not agree, or if you agree but have comments or suggestions for the draft Implementation Guidance, please provide your recommendation and explanation.

5. The SDT believes proposed CIP-012-1 provides entities with flexibility to meet the reliability objectives in a cost effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost effective approaches, please provide your recommendation and, if appropriate, technical justification.

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim	3	RF	FirstEnergy Corporation	Aaron Ghdooshim	FirstEnergy - FirstEnergy Corporation	4	RF
					Aubrey Short	FirstEnergy - FirstEnergy Corporation	1	RF
					Theresa Ciancio	FirstEnergy - FirstEnergy Corporation	3	RF
					Robert Loy	FirstEnergy - FirstEnergy Solutions	5	RF
					Ann Ivanc	FirstEnergy - FirstEnergy Solutions	6	RF
Brandon McCormick	Brandon McCormick		FRCC	FMPA	Tim Beyrle	City of New Smyrna Beach Utilities Commission	4	FRCC
					Jim Howard	Lakeland Electric	5	FRCC
					Lynne Mila	City of Clewiston	4	FRCC
					Javier Cisneros	Fort Pierce Utilities Authority	3	FRCC
					Randy Hahn	Ocala Utility Services	3	FRCC
					Don Cuevas	Beaches Energy Services	1	FRCC
					Jeffrey Partington	Keys Energy Services	4	FRCC
					Tom Reedy	Florida Municipal Power Pool	6	FRCC
					Steven Lancaster	Beaches Energy Services	3	FRCC

					Mike Blough	Kissimmee Utility Authority	5	FRCC
					Chris Adkins	City of Leesburg	3	FRCC
					Ginny Beigel	City of Vero Beach	3	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
Seattle City Light	Ginette Lacasse	1,3,4,5,6	WECC	Seattle City Light Ballot Body	Pawel Krupa	Seattle City Light	1	WECC
					Hao Li	Seattle City Light	4	WECC
					Bud (Charles) Freeman	Seattle City Light	6	WECC
					Mike Haynes	Seattle City Light	5	WECC
					Michael Watkins	Seattle City Light	1,4	WECC
					Faz Kasraie	Seattle City Light	5	WECC
					John Clark	Seattle City Light	6	WECC
					Tuan Tran	Seattle City Light	3	WECC
					Laurrie Hammack	Seattle City Light	3	WECC
Southern Company - Southern Company Services, Inc.	Pamela Hunter	1,3,5,6	SERC	Southern Company	Katherine Prewitt	Southern Company Services, Inc.	1	SERC
					Joel Dembowski	Southern Company - Alabama Power Company	3	SERC
					William D. Shultz	Southern Company Generation	5	SERC
					Jennifer G. Sykes	Southern Company Generation	6	SERC

						and Energy Marketing		
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,8,9,10	NPCC	RSC no Dominion, NextEra and HQ	Guy V. Zito	Northeast Power Coordinating Council	10	NPCC
					Randy MacDonald	New Brunswick Power	2	NPCC
					Wayne Sipperly	New York Power Authority	4	NPCC
					Glen Smith	Entergy Services	4	NPCC
					Brian Robinson	Utility Services	5	NPCC
					Alan Adamson	New York State Reliability Council	7	NPCC
					Edward Bedder	Orange & Rockland Utilities	1	NPCC
					David Burke	Orange & Rockland Utilities	3	NPCC
					Michele Tondalo	UI	1	NPCC
					Laura Mcleod	NB Power	1	NPCC
					David Ramkalawan	Ontario Power Generation Inc.	5	NPCC
					Helen Lainis	IESO	2	NPCC
					Michael Schiavone	National Grid	1	NPCC
					Michael Jones	National Grid	3	NPCC
					Michael Forte	Con Ed - Consolidated Edison	1	NPCC
					Peter Yost	Con Ed - Consolidated Edison Co. of New York	3	NPCC
					Sean Cavote	PSEG	4	NPCC

					Kathleen Goodman	ISO-NE	2	NPCC
					Paul Malozewski	Hydro One Networks, Inc.	3	NPCC
					Quintin Lee	Eversource Energy	1	NPCC
					Gregory Campoli	New York Independent System Operator	2	NPCC
					Dermot Smyth	Con Ed - Consolidated Edison Co. of New York	1,5	NPCC
					Dermot Smyth	Con Ed - Consolidated Edison Co. of New York	1,5	NPCC
					Salvatore Spagnolo	New York Power Authority	1	NPCC
					Shivaz Chopra	New York Power Authority	6	NPCC
					David Kiguel	Independent	NA - Not Applicable	NPCC
Midwest Reliability Organization	Russel Mountjoy	10		MRO NSRF	Joseph DePoorter	Madison Gas & Electric	3,4,5,6	MRO
					Larry Heckert	Alliant Energy	4	MRO
					Amy Casucelli	Xcel Energy	1,3,5,6	MRO
					Michael Brytowski	Great River Energy	1,3,5,6	MRO
					Jodi Jensen	Western Area Power Administratino	1,6	MRO
					Kayleigh Wilkerson	Lincoln Electric System	1,3,5,6	MRO
					Mahmood Safi	Omaha Public Power District	1,3,5,6	MRO
					Brad Parret	Minnesota Power	1,5	MRO
					Terry Harbour	MidAmerican Energy Company	1,3	MRO

					Tom Breene	Wisconsin Public Service	3,5,6	MRO
					Jeremy Volls	Basin Electric Power Coop	1	MRO
					Kevin Lyons	Central Iowa Power Cooperative	1	MRO
					Mike Morrow	Midcontinent Independent System Operator	2	MRO
Dominion - Dominion Resources, Inc.	Sean Bodkin	6		Dominion	Connie Lowe	Dominion - Dominion Resources, Inc.	3	NA - Not Applicable
					Lou Oberski	Dominion - Dominion Resources, Inc.	5	NA - Not Applicable
					Larry Nash	Dominion - Dominion Virginia Power	1	NA - Not Applicable
Colorado Springs Utilities	Shannon Fair	1,3,5,6		Colorado Springs Utilities	Jeff Icke	Colorado Springs Utilities	5	WECC
					Hilary Dobson	Colorado Springs Utilities	3	WECC
					Brandon Ware	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
					Steve Keller	Soutwest Power Pool Inc	2	SPP RE
					Sean Simpson	Board of Public Utilities, City of Mcpherson, Kansas	NA - Not Applicable	SPP RE
					louis Guidry	Cleco	1,3,5,6	SPP RE

Associated Electric Cooperative, Inc.	Todd Bennett	3		AECI	Michael Bax	Central Electric Power Cooperative (Missouri)	1	SERC
					Adam Weber	Central Electric Power Cooperative (Missouri)	3	SERC
					Stephen Pogue	M and A Electric Power Cooperative	3	SERC
					William Price	M and A Electric Power Cooperative	1	SERC
					Jeff Neas	Sho-Me Power Electric Cooperative	3	SERC
					Peter Dawson	Sho-Me Power Electric Cooperative	1	SERC
					Mark Ramsey	N.W. Electric Power Cooperative, Inc.	1	NPCC
					John Stickley	NW Electric Power Cooperative, Inc.	3	SERC
					Ted Hilmes	KAMO Electric Cooperative	3	SERC
					Walter Kenyon	KAMO Electric Cooperative	1	SERC
					Kevin White	Northeast Missouri Electric Power Cooperative	1	SERC
					Skyler Wiegmann	Northeast Missouri Electric Power Cooperative	3	SERC
					Ryan Ziegler	Associated Electric Cooperative, Inc.	1	SERC
					Brian Ackermann	Associated Electric	6	SERC

						Cooperative, Inc.		
					Brad Haralson	Associated Electric Cooperative, Inc.	5	SERC

1. Requirement R1: The SDT drafted CIP-012-1 Requirement R1 for the Responsible Entity to implement one or more documented plan(s) to mitigate the risk of the unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring data while being transmitted between any Control Centers. Do you agree with this revision? If not, please provide the basis for your disagreement and an alternate proposal.

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion

Answer	No
Document Name	

Comment

R1.2 needs to be modified to reflect the comments in question 4 below.

“On page 5 under section “Identification of Where Security Protection is Applied by the Responsible Entity”, language should be added to address the situation where a Responsible Entity does not manage either end of a communication link, indicating that this Responsible Entity does not have compliance obligations to R1.2.”

Likes 0	
Dislikes 0	

Response

Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,4,5 - RF

Answer	No
Document Name	

Comment

The requirement as written does not provide clear threshold on the type of Control Centers that should be in scope for this standard, i.e. does this requirement apply to high/medium impact BES Cyber Systems, or it also applies to low impact BES Cyber System. Please clarify. Please also consider how to incorporate the scoping criteria into CIP-002 standard.

Likes 0	
Dislikes 0	

Response

Marty Hostler - Northern California Power Agency - 5

Answer	No
Document Name	

Comment

This standard is unnecessary IRO-010 and TOP-003 already require a mutually agreeable security protocol.

Likes 0	
Dislikes 0	

Response

Darnez Gresham - Darnez Gresham On Behalf of: Annette Johnston, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Darnez Gresham

Answer	No
Document Name	

Comment

We support the MRO NSRF comments and add these. One, until the definition of Control Center is set, we will vote no due to uncertain scope for this requirement. Two, "security protection used to mitigate risk" is too ambiguous for an enforceable standard. We respect the SDT's challenge in writing language that is not overly prescriptive but yet enforceable. However, we respectfully request SDT to consider including two concepts in R1. First concept is to include clarity on currently in place ICCP. The Requirement states "while being transmitted between any Control Centers." The draft Implementation Guidance has content talking about "both ends of the link" but doesn't enlighten on what the expectations are for the data while on the link. We are concerned with latency (primarily for generation control) if secure encryption is expected over the ICCP. Also, it is our understanding the secure ICCP may not be widely implemented. Second concept is to include examples that include but are not limiting for security protection.

Likes 1	Central Hudson Gas & Electric Corp., 1, Pace Frank
Dislikes 0	

Response

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5

Answer	No
Document Name	

Comment

Given this ballot is concurrently open with the Control Center definition revision, NV Energy cannot vote affirmative for this iteration of CIP-012-1, until there is further clarity in the Control Center definition, or the definition is approved. Additionally, NV Energy has concerns with the implementation of security protections associated with its multiple ICCP links. The reference documentation of the proposed Standard assumes an “ease” for installation of “secure ICCP”, but previous regional studies of such protections have proven unfeasible and costly.

Likes 0	
Dislikes 0	

Response

James Anderson - CMS Energy - Consumers Energy Company - 1	
Answer	No
Document Name	
Comment	
The requirement as written does not provide clear threshold on the type of Control Centers that should be in scope for this standard, i.e. does this requirement apply to high/medium impact BES Cyber Systems, or it also applies to low impact BES Cyber System. Please clarify. Please also consider how to incorporate the scoping criteria into CIP-002 standard.	
Likes 0	
Dislikes 0	
Response	
Ellen Oswald - Midcontinent ISO, Inc. - 2	
Answer	No
Document Name	
Comment	
The statement for Real-time monitoring does not include control data here. Again for clarification and consistency is control going to be removed from all the referencing within CIP-012 or added to all references of Real-time monitoring requirements.	
Likes 0	
Dislikes 0	
Response	
Brandon McCormick - Brandon McCormick On Behalf of: Ginny Beigel, City of Vero Beach, 3; Lynne Mila, City of Clewiston, 4; Mike Blough, Kissimmee Utility Authority, 5, 3; Tom Reedy, Florida Municipal Power Pool, 6; - Brandon McCormick, Group Name FMPA	
Answer	No
Document Name	
Comment	
FMPA agrees with the following comments from Lakeland Electric: Real-time Assessments lists a number of specific inputs that should be considered for both “Real-time Assessment (RTA) and Real-time monitoring (RTm) data.” There may be an overly stringent audit approach taken that would require consideration of both RTA AND RTm data for proof that an entity provided adequate protections. If there is a distinction between data used for the RTA and data used for RTm, please provide clarification of the	

expectation. We recommend consideration of the use of the inputs in the RTA NERC term with a caveat that Entities may choose to protect additional data if they feel the need to expand the scope.

From the RTA definition: The assessment shall reflect applicable inputs including, but not limited to: load, generation output levels, known Protection System and Special Protection System status or degradation, Transmission outages, generator outages, Interchange, Facility Ratings, and identified phase angle and equipment limitations.

While we recognize that TOP/GOP are doing monitoring of their own systems, the Functional Model does not include the term monitoring in the list of the functions they are performing in real-time. The TOP/GOP functions include “providing real time operational information” or “real time operating information” to the BA/RC.

The term “any Control Centers” may be overly broad as it seems more reasonable for the standards to apply to High and Medium Impact Control Centers. It seems more likely that the Control Centers that meet the low impact rating for CIP-002 Attachment 1 Criteria for Low Impact found in section 3 would be transmitting information via the ICCP network. The RC should be required to plan for the encryption of that data on behalf of the Entities under their direction/control. I believe that some of the “Low Impact Control Centers” may not be required to have a backup control center, especially if they are operating out of a control house at a substation or control room at a generating plant.

Also, the VRF/VSL still contains language related to CIP Exceptional Circumstances which was part of R2 which was struck from the standard.

Likes 0	
Dislikes 0	

Response

Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC

Answer	No
Document Name	

Comment

While Tri-State agrees with the language of Requirement R1, we are concerned that there could be a possible violation if logical protections (encryption) were to temporarily fail. Is that the intent of the SDT? The removal of the CIP Exceptional Circumstance that was in R2 no longer provides the exception from potential noncompliance if either entity's protections fail due to catastrophic event. Tri-State would like for the CIP Exceptional Circumstance exclusion to be added back to the standard.

Additionally, if we use encryption as our primary method to meet this requirement and it fails, can we rely solely on physical protections identified and documented in our plans as a backup protection method to satisfy the intent of the standard?

Likes 0	
Dislikes 0	

Response	
Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	
Comment	
This standard is unnecessary. IRO-010 and TOP-003 already require a mutually agreeable security protocol.	
Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	
CenterPoint Energy Houston Electric, LLC (“CenterPoint Energy”) does not agree with the revision and suggests adding the phrase “except under CIP Exceptional Circumstances” to the first sentence to be consistent with the earlier version. CenterPoint Energy recommends changing the first sentence to: “The Responsible Entity shall implement one or more documented plan(s) to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring data while being transmitted between any Control Centers, except under CIP Exceptional Circumstances.”	
Likes 0	
Dislikes 0	
Response	
Heather Morgan - EDP Renewables North America LLC - 5	
Answer	No
Document Name	
Comment	
There is concern about the overlap between CIP-012 and TOP-003-3/IRO-010-2. These Standards dictate what generators must comply with from our RC, BA, and TOP in the way of data communication. As a generator, we must comply with our TOP-003 and IRO-010 instructions for data	

communication. Should these standards be combined? Will the RC, BA, and TOP take responsibility to ensure security of the data being transmitted on their equipment that we are required to use? In the current language, there is a lack of ownership responsibility. For 1.3, the RC, BA, and TOP (as the authorizing entities that own the equipment and instruct generators on how to comply for IRO-010 and TOP-003) should be responsible (for identifying not only their RC, BA, and TOP) responsibilities, but the Generator Operator's responsibilities as well.	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
PacifiCorp supports MEC's comments and adds the following: In November 2005, it was decided that all Reliability Transmission Controllers (RTCs, now called RCs) would need to have Secure ICCP implemented by October 2006, and that all connecting utilities would need to have Secure ICCP by October 2008. Encryption between routers was discussed, but some utilities managed their own edge routers and others were managed by AT&T therefore, coordination between entities could not be secured. Eventually Secure ICCP was removed from the Data Exchange/EMS Work Group (DEMSWG) agendas. There is no awareness of any WECC utilities which are making use of Secure ICCP today, and only a limited number utilities have the capability. The WECC Data Exchange/EMS Work Group (DEMSWG) worked with vendors to perform inter-operability testing and also train utilities in how to obtain and install certificates. This effort is referenced in comments for item 3 below. Please provide additional clarity where ICCP is used for Real-time Assessment and Real-time monitoring data being transmitted between any Control Centers owned or operated by different Responsible Entities. (Please note the distinction between ICCP and Secure ICCP used above)	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	

Comment
We support the MRO NSRF comments and add these. One, until the definition of Control Center is set, we will vote no due to uncertain scope for this requirement. Two, "security protection used to mitigate risk" is too ambiguous for an enforceable standard. We respect the SDT's challenge in writing language that is not overly prescriptive but yet enforceable. However, we respectfully request SDT to consider including two concepts in R1. First concept is to include clarity on currently in place ICCP. The Requirement states "while being transmitted between any Control Centers." The draft Implementation Guidance has content talking about "both ends of the link" but doesn't enlighten on what the expectations are for the data while on the link. We are concerned with latency (primarily for generation control) if secure encryption is expected over the ICCP. Also, it is our understanding the secure ICCP may not be widely implemented. Second concept is to include examples that include but are not limiting for security protection.

Likes 0	
Dislikes 0	

Response

Warren Cross - ACES Power Marketing - 1,3,4,5 - MRO,WECC,Texas RE,SERC,SPP RE,RF	
Answer	No
Document Name	

Comment
The SDT team has done a good job of responding to industry comments regarding CIP-012. Does an entity need to draft a new plan to mitigate these areas of concerns: - security protection used to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers; - where the Responsible Entity applied security protection for transmitting Real-time Assessment and Real-time monitoring data between Control Centers; - The responsibilities of each Responsible Entity for applying security protection to the transmission of Real-time Assessment and Real-time monitoring data between Control Centers that are owned or operated by different Responsible Entities. Does not the current set of standards address those additional vulnerabilities in the entity’s IT Security Plan? That current plan should be updated to include these additional risks, threats and integrated solution(s) that are already by performed by the entity.

Likes 0	
Dislikes 0	

Response

Wendy Center - U.S. Bureau of Reclamation - 5	
Answer	No
Document Name	
Comment	

Reclamation disagrees that having a plan adds to the reliability of protecting data used for Real-time Assessment and Real-time monitoring. A plan is an unwarranted layer of compliance that is not needed. Reclamation recommends replacing the term “plan” with “process” and rewriting R1 and its parts as follows:

- R1. Each Responsible Entity shall implement one or more documented processes to mitigate the risk of unauthorized disclosure or modification of BES Data being transmitted between any Control Centers. This requirement excludes oral and non-electronic communications.
    - R1.1. Identify the security protection used to mitigate the risk of unauthorized disclosure of BES Data being transmitted between Control Centers;
    - R1.2. Identify where the Responsible Entity applied security protection for transmitting BES Data between Control Centers; and
    - R1.3. Identify the responsibilities of each Responsible Entity whose Control Center(s) are involved in the transmission of BES Data.

Reclamation also recommends adding the following definition to the NERC Glossary of Terms:

- BES Data: BES reliability operating services information affecting Operational Planning Analysis, Real-time Assessments, and Real-time monitoring.

Likes 0	
Dislikes 0	
Response	

Jamie Prater - Entergy - 5	
Answer	No
Document Name	
Comment	

Comments: The deletion of R2 removed the exemption for “except under CIP Exceptional Circumstances," however the CIP Exceptional Circumstances language still exists in the VSL/VRF tables. The CIP Exceptional Circumstance language should be explicitly added to the R1 requirement to align with the VSL/VRF, and clearly indicate the intent of the requirement.

Likes 0	
Dislikes 0	
Response	

Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 3

Answer	No
Document Name	
Comment	
PNM agrees with FMPA's comment which stated “... the VRF/VSL still contains language related to CIP Exceptional Circumstances which was part of R2 which was struck from the standard.”	
Likes 0	
Dislikes 0	
Response	
Laurie Williams - PNM Resources - Public Service Company of New Mexico - 1	
Answer	No
Document Name	
Comment	
PNM agrees with FMPA's comment which stated “... the VRF/VSL still contains language related to CIP Exceptional Circumstances which was part of R2 which was struck from the standard."	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino	

Answer	Yes
Document Name	
Comment	

Real-time monitoring is not a defined term, the R in Real-time should not be capitalized. We are still concerned that coordination between control centers may result in compromises that may not satisfy the needs of the entities involved.

Likes 0	
Dislikes 0	
Response	

Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF

Answer	Yes
Document Name	
Comment	

The drafting team has done a good job of responding to industry comments. The NSRF would like to offer the following two items:

1) The Standards Efficiency group within NERC is working towards actionable Standards and removing the layers of compliance that do not promote reliability. The NSRF recommends for R1 that entities not be required to have a plan, but have an actionable Requirement to implement. NSRF suggests the following R1 wording:

"The Responsible Entity shall mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring data while being transmitted between any Control Centers. This requirement excludes oral communications. Responsible Entities shall document:

- security protection used to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers;
- where the Responsible Entity applied security protection for transmitting Real-time Assessment and Real-time monitoring data between Control Centers;
- The responsibilities of each Responsible Entity for applying security protection to the transmission of Real-time Assessment and Real-time monitoring data between Control Centers that are owned or operated by different Responsible Entities.

2) NERC has issued for comment the definition for Control Center during the third draft of CIP-012-1. The definition of terms late in the drafting/balloting process of a Standard is not the right time to consider a definition change as this may impact the Standard being considered during the late rounds of balloting. The NSRF recommends that defined terms be offered up in the early stages of drafting and balloting of Standards.

Likes 0	
Dislikes 0	

Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	Yes
Document Name	
Comment	
City Light supports SRP comments	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
See MRO NSRF comments.	
Likes 0	
Dislikes 0	
Response	
Shannon Fair - Colorado Springs Utilities - 1,3,5,6, Group Name Colorado Springs Utilities	
Answer	Yes
Document Name	
Comment	
CSU agrees the data should be protected. CSU also agrees the protections for the data in scope must ensure the data has not been modified, and that FERC directed NERC to “specify how the confidentiality, integrity, and availability of each type of bulk electric system data should be protected while it is being transmitted.” However, CSU takes exception to the extent the proposed standard requires the data in scope to be protected. FERC Order 822 states on page 36, “ we recognize that not all communication network components and data pose the same risk to bulk electric system reliability and may not require the same level of protection.” However, the proposed standard applies the same criteria of protection against unauthorized disclosure across all of the data within the defined scope. CSU does not agree viewing of the Real-time Assessment and Real-time monitoring and control data without context will decrease the reliable operation of the BES and asserts confidentiality does not need to be protected for all data under this scope. Along with this, CSU would like a clarification of how the SDT defines Real-Time Assessment Data.	

Additionally, CSU recognizes the SDT is not specifying the controls used to protect confidentiality and integrity. However, the only method available to achieve the proposed required objective is to implement encryption. FERC Order 822 states on page 39, “it is reasonable to conclude that any lag in communication speed resulting from implementation of protections [encryption technologies] should only be measureable on the order of milliseconds and, therefore, will not adversely impact Control Center communications,” but CSU asserts this statement only refers to a single data stream. It is unknown what encryption will do when dealing with multiple data streams being transmitted at once, from one to many points, not only to the latency added for the reliable operation of the BES, but also to the computing resources.

Likes 0	
Dislikes 0	

Response

Thomas Breene - WEC Energy Group, Inc. - 3

Answer	Yes
Document Name	

Comment

While we support the changes to the standard, we are concerned that there may be unintended consequences if the Control Center definition is approved as proposed and urge the SDT to proceed with caution.

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

While Duke Energy has no immediate concerns regarding the scope of R1, we do have concerns regarding the proposed definition of Control Center which is included in this project. We have submitted our comments on the proposed definition separately, and will not repeat them here. However, the definition of Control Center is directly related to the overall scope of CIP-012, and if we have some clarifying concerns with the definition, those same concerns are inherent to the proposed CIP-012. We suggest the drafting team consider the procedural effects of balloting these two related items separately, when they are so directly related.

Likes 0	
Dislikes 0	

Response

Vivian Vo - APS - Arizona Public Service Co. - 3

Answer	Yes
Document Name	CIP-012-1_Draft 3_AZPS Comments-Question 1.docx
Comment	
Please see the attached file for Arizona Public Service Co.'s comments to Question 1.	
Likes 0	
Dislikes 0	
Response	
John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1	
Answer	Yes
Document Name	
Comment	
No Comment	
Likes 0	
Dislikes 0	
Response	
Jack Cashin - American Public Power Association - 4	
Answer	Yes
Document Name	
Comment	
no comment	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	

Comment
Yes, with comments. Some of Southern Company's partner utilities do not currently use a VPN for their data connections – this will require Southern to engage in discussions and potentially renegotiate contract terms regarding these connections. We recognize that other utilities will be held to the same standard and, therefore, will be motivated to work toward maintaining compliance. We recognize this as something we will need to spend time to address.

Likes 0	
Dislikes 0	

Response

Russell Martin II - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	

Comment
SRP agrees the data should be protected. SRP also agrees the protections for the data in scope must ensure the data has not been modified, and that FERC directed NERC to "specify how the confidentiality, integrity, and availability of each type of bulk electric system data should be protected while it is being transmitted." However, SRP takes exception to the extent the proposed standard requires the data in scope to be protected. FERC Order 822 states on page 36, "…we recognize that not all communication network components and data pose the same risk to bulk electric system reliability and may not require the same level of protection." However, the proposed standard applies the same criteria of protection against unauthorized disclosure across all of the data within the defined scope. SRP does not agree viewing of the Real-time Assessment and Real-time monitoring and control data without context will decrease the reliable operation of the BES and asserts confidentiality does not need to be protected for all data under this scope. Along with this, SRP would like a clarification of how the SDT defines Real-Time Assessment Data. Additionally, SRP recognizes the SDT is not specifying the controls used to protect confidentiality and integrity. However, the only method available to achieve the proposed required objective is to implement encryption. FERC Order 822 states on page 39, "it is reasonable to conclude that any lag in communication speed resulting from implementation of protections [encryption technologies] should only be measureable on the order of milliseconds and, therefore, will not adversely impact Control Center communications," but SRP asserts this statement only refers to a single data stream. It is unknown what encryption will do when dealing with multiple data streams being transmitted at once, from one to many points, not only to the latency added for the reliable operation of the BES, but also to the computing resources.

Likes 0	
Dislikes 0	

Response

Kristine Ward - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
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	
Aaron Austin - AEP - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Faz Kasraie - Seattle City Light - 5 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1,3,5 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Douglas Johnson - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 3, Group Name FirstEnergy Corporation	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrey Komissarov - Andrey Komissarov On Behalf of: Jerome Gobby, Sempra - San Diego Gas and Electric, 3, 5, 1; - Andrey Komissarov	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Russell Noble - Cowlitz County PUD - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion, NextEra and HQ	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	
Document Name	
Comment	
AECI supports comments provided by NRECA	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	

Document Name	
Comment	
Texas RE appreciates the SDT's efforts to develop a workable data security standard. In particular, Texas RE believes that the SDT's various revisions have substantially improved the proposed CIP-012-1 Standard from the initial version. Despite these improvements, Texas RE remains concerned that the proposed Standard, as currently drafted, is not sufficiently clear that in identifying both the security protections used to mitigate the risk of unauthorized disclosures and the locations where the Responsible Entities applied such protections, Responsible Entities will need to protect both data throughout the transmission process, as well as communications links. That is, Texas RE continues to believe that FERC Order No, 822 contemplated both physical protection of communications links and additional protections for data to ensure there is adequate "security protection used to mitigate the risk of unauthorized disclosure or modification" of data while being transmitted between Control Centers. As such, Texas RE recommends inserting the phrase "including protections for communications links and data" into the proposed CIP-012-1 R1.1 so that it reads "[i]dentification of security protection, including protections for communications links and data, used to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers." Texas RE continues to be concerned that Operations Planning Analysis (OPA) data is not included in CIP-012-1. Texas RE noticed the Violation Time Horizon is for Operations Planning. Since the SDT has indicated reasons for excluding OPA data, should the relevant Violation Time Horizon be Real-time Operation?	
Likes 0	
Dislikes 0	
Response	

2. Implementation Plan: The SDT established the Implementation Plan to make the standard effective the first day of the first calendar quarter that is twenty-four (24) calendar months after the effective date of the applicable governmental authority's order approving the standard, or as otherwise provided for by the applicable governmental authority. Do you agree with this proposal? If you think an alternate implementation time period is needed, please provide a detailed explanation of actions and time needed to meet the implementation deadline.

Russell Martin II - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	

Comment

Overall, SRP does not agree with twenty-four (24) calendar months for the implementation of Requirements R1, as R1 and R2 from the second draft have been merged. Although SRP recognizes the SDT is not specifying the controls to be used to protect confidentiality and integrity, the only examples provided in the implementation guidance includes encryption. If there are other methods available to achieve the security objective, SRP asks the SDT to provide them. However, the only method available to achieve the proposed required objective, on the ICCP network, is to implement encryption. As FERC order 822 states on page 37, "if several registered entities have joint responsibility for a cryptographic key management system used between their respective Control Centers, they should have the prerogative to come to a consensus on which organization administers that particular key management system." Furthermore, the FERC order states on page 38, "While responsible entities are required to exchange real-time and operational planning data necessary to operate the bulk electric system using mutually agreeable security protocols, there is no technical specification for how this transfer of information should incorporate mandatory security controls." These are activities and specifications that must be created and agreed upon by all registered entities involved in the data transfer. As such the timeline is reliant on registered entities working together on a common solution and would not be achievable within 24 calendar months.

Additionally, if encryption fails, SRP would lose Real-time Assessment and Real-time monitoring and control data. There are many opportunities for encryption to fail that must be addressed. The implementation of encryption requires a pilot to truly understand and address the mechanisms of failure, the impacts encryption would cause on the exchange of the data, and the computing resources required. A pilot also requires a great amount of coordination to execute, not only within the industry, but may also include carriers, vendors, and possibly third-party encryption key program managers.

Because of the aforementioned reasons and concerns, SRP is recommending a phased implementation for CIP-012-1. A 24 month implementation is appropriate, but only for Requirement R1. The 24 months for R1 would provide time to coordinate and create an industry-wide solution. SRP is proposing the SDT include an additional 12 months for the plan implementation aspect of Requirement R1. The additional 12 months would be used for a pilot and course correction if needed, in addition to understanding, formulating, and executing maintenance strategies.

Likes 0	
Dislikes 0	

Response

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	

Comment	
Until the security protections scope is clearer and the definition of Control Center is final, it is not possible to determine if 24 months is adequate.	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
PacifiCorp support MEC's comments and add the following: Until the definition of Control Center is final and clarity is added where ICCP is used for Real-time Assessment and Real-time monitoring data being transmitted between any Control Centers owned or operated by different Responsible Entities, it is not possible to determine if 24 months is adequate. (Please note the distinction between ICCP and Secure ICCP used in question 2 above)	
Likes 0	
Dislikes 0	
Response	
Russell Noble - Cowlitz County PUD - 3	
Answer	No
Document Name	
Comment	
Cowlitz PUD supports the comments submitted by the Bonneville Power Administration.	
Likes 0	
Dislikes 0	
Response	
Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	

Comment	
See Response to Question 1.	
Likes 0	
Dislikes 0	
Response	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	No
Document Name	
Comment	
Recommend 36 months for 1) review and 2) develop new contract and 3) budgetary cycles 4) Implementation cycles (planned outages, etc.)	
Likes 0	
Dislikes 0	
Response	
Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	No
Document Name	
Comment	
Tri-State anticipates implementation of CIP-012 could be extremely burdensome and would recommend increasing the implementation period to 36 months. Depending on the number of connections to other entities, the negotiation process could take some significant resources and time. Tri-State suggests the SDT send a survey to industry requesting feedback to gauge the number of connections to other entities industry has and the amount of time entities expect they will need to implement CIP-012.	
Likes 0	
Dislikes 0	
Response	
Ellen Oswald - Midcontinent ISO, Inc. - 2	
Answer	No
Document Name	

Comment
Concerns about the contracts with third parties for carriers used between applicable control centers. If they are dedicated or shared circuits based on the implementation guidance document this should not be an issue until it is actually put into practical use.

Likes 0	
Dislikes 0	

Response

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5

Answer	No
Document Name	

Comment
Without further clarity involving security protections of the data (i.e. ICCP protections) NV Energy is unable to determine if the 24 calendar months is sufficient.

Likes 0	
Dislikes 0	

Response

Darnez Gresham - Darnez Gresham On Behalf of: Annette Johnston, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Darnez Gresham

Answer	No
Document Name	

Comment
Until the security protections scope is clearer and the definition of Control Center is final, it is not possible to determine if 24 months is adequate.

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
Duke Energy suggests a staggered implementation plan for CIP-012 specifically concerning coordination with neighboring entities. We consider it possible for an entity to gather necessary data, convening of internal work groups, and drafting of security protection plans in the proposed 24 month Implementation Plan. However, we feel that the coordination with other entities that will be necessary for R1.3 will take longer than the proposed 24 months, especially with internal work already taking place. We recommend the drafting team consider a staggered implementation plan for internal work (18 months) compared to external coordination work (36 months). We feel that this amount of time will is necessary to implement all aspects of the proposed standard.

Likes 0	
Dislikes 0	

Response

Marty Hostler - Northern California Power Agency - 5

Answer	No
Document Name	

Comment
See Response to Question 1.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment
CSU does not agree with twenty-four (24) calendar months for the implementation of Requirements R1, as R1 and R2 from the second draft have been merged. Although CU recognizes the SDT is not specifying the controls to be used to protect confidentiality and integrity, the only examples provided in the implementation guidance includes encryption. If there are other methods available to achieve the security objective, SRP asks the SDT to provide them. However, the only method available to achieve the proposed required objective, on the ICCP network, is to implement encryption. As FERC order 822 states on page 37, “if several registered entities have joint responsibility for a cryptographic key management system used between their respective Control Centers, they should have the prerogative to come to a consensus on which organization administers that particular key management system.” Furthermore, the FERC order states on page 38, “While responsible entities are required to exchange real-time and operational planning data necessary to operate the bulk electric system using mutually agreeable security protocols, there is no technical specification for how this transfer of information should incorporate mandatory security controls.” These are activities and specifications that must be created and agreed upon by all registered entities involved in the data transfer. As such the timeline is reliant on registered entities working together on a common solution and would not be achievable within 24 calendar months.

Additionally, if encryption fails, CSU would lose Real-time Assessment and Real-time monitoring and control data. There are many opportunities for encryption to fail that must be addressed. The implementation of encryption requires a pilot to truly understand and address the mechanisms of failure, the impacts encryption would cause on the exchange of the data, and the computing resources required. A pilot also requires a great amount of coordination to execute, not only within the industry, but may also include carriers, vendors, and possibly third-party encryption key program managers.

Because of the aforementioned reasons and concerns, CSU is recommending a phased implementation for CIP-012-1. A 24 month implementation is appropriate, but only for Requirement R1. The 24 months for R1 would provide time to coordinate and create an industry-wide solution. CSU is proposing the SDT include an additional 12 months for the plan implementation aspect of Requirement R1. The additional 12 months would be used for a pilot and course correction if needed, in addition to understanding, formulating, and executing maintenance strategies.

Likes 0	
Dislikes 0	

Response

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

BPA appreciates the increase to 24 months but recommends 36 months due to BPA’s large amount of applicable data, access to funds and budget cycle, and resources to perform work required.

Likes 0	
Dislikes 0	

Response

Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body

Answer	No
Document Name	

Comment

City Light supports SRP comments

Likes 0	
Dislikes 0	

Response

Patricia Lynch - NRG - NRG Energy, Inc. - 5,6

Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brandon McCormick - Brandon McCormick On Behalf of: Ginny Beigel, City of Vero Beach, 3; Lynne Mila, City of Clewiston, 4; Mike Blough, Kissimmee Utility Authority, 5, 3; Tom Reedy, Florida Municipal Power Pool, 6; - Brandon McCormick, Group Name FMPA	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 5	
Answer	Yes
Document Name	
Comment	
Reclamation supports a 24-month implementation period.	
Likes 0	
Dislikes 0	
Response	
Warren Cross - ACES Power Marketing - 1,3,4,5 - MRO,WECC,Texas RE,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	

No comment.

Likes 0	
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	Yes
Document Name	

Comment

Yes, without additional comment.

Likes 0	
Dislikes 0	

Response

Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE

Answer	Yes
Document Name	

Comment

Due to the time and cost of acquiring and implementing needed technological solutions and the coordination that will be required between Responsible Entities, a 24 month implementation period would be the minimal amount of time needed to properly implement the proposed Requirements.

Likes 0	
Dislikes 0	

Response

Chris Scanlon - Exelon - 1

Answer	Yes
Document Name	

Comment

24 months should be the minimum implementation time used, no shorter.

Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
See MRO NSRF comments.	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
24 months allows the Responsible Entity sufficient time to both develop and successfully implement the plan. This would include coordination with neighboring entities and potentially adding new controls to the communication links.	
Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jamie Prater - Entergy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion, NextEra and HQ	
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	
Heather Morgan - EDP Renewables North America LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Teresa Cantwell - Lower Colorado River Authority - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrey Komissarov - Andrey Komissarov On Behalf of: Jerome Gobby, Sempra - San Diego Gas and Electric, 3, 5, 1; - Andrey Komissarov	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Anderson - CMS Energy - Consumers Energy Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 3	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 3, Group Name FirstEnergy Corporation	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Douglas Johnson - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Adrian Andreoiu - BC Hydro and Power Authority - 1,3,5 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thomas Breene - WEC Energy Group, Inc. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Faz Kasraie - Seattle City Light - 5 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Austin - AEP - 3	

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	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Kristine Ward - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jack Cashin - American Public Power Association - 4	
Answer	
Document Name	
Comment	
The proposed standard and implementation plan are silent on physical security for the equipment being used to provide the data protection. For example, physical security protection for a router located in another Entity's facility. Trouble shooting such issues could affect the implementation schedule.	
Likes 0	
Dislikes 0	
Response	
John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1	
Answer	
Document Name	
Comment	
Tacoma Power supports comments provided by APPA.	
Likes 0	

Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	
Document Name	
Comment	
AECI supports comments provided by NRECA	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	
Document Name	
Comment	
The proposed standard and implementation plan are silent on physical security for the equipment being used to provide the data protection. For example, protection for a router that is located in an other Entities facility	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	
Document Name	
Comment	
WECC has heard concerns voiced that a 24 calendar month implementation plan is not enough time to implemnt the technical solution, however, a alternative time frame has not been suggested.	
Likes 0	
Dislikes 0	

Response

3. The SDT modified the draft Technical Rationale and Justification for CIP-012 to assist in understanding the technology and technical requirements in the Reliability Standard. It also contains information on the SDT's intent in drafting the requirements. Do you agree with the technology and technical requirements in the draft Technical Rationale and Justification? If you do not agree, or if you agree but have comments or suggestions for the draft Technical Rationale and Justification, please provide your recommendation and explanation.

Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,4,5 - RF

Answer	No
Document Name	

Comment

To be consistent with other CIP standards, please combine Technical Rational and Justification document with the Implementation Guidance document and then incorporate the new document into the draft standard. Please clarify that CIP-012 is a standalone standard that is not associated with all the other CIP standards.

Likes 0	
Dislikes 0	

Response

Marty Hostler - Northern California Power Agency - 5

Answer	No
Document Name	

Comment

See Response to Question 1.

Likes 0	
Dislikes 0	

Response

Darnez Gresham - Darnez Gresham On Behalf of: Annette Johnston, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Darnez Gresham

Answer	No
Document Name	

Comment

We support MRO NSRF comments.

Likes 0	

Dislikes 0	
Response	
James Anderson - CMS Energy - Consumers Energy Company - 1	
Answer	No
Document Name	
Comment	
To be consistent with other CIP standards, please combine Technical Rational and Justification document with the Implementation Guidance document and then incorporate the new document into the draft standard. Please clarify that CIP-012 is a standalone standard that is not associated with all the other CIP standards.	
Likes 0	
Dislikes 0	
Response	
Ellen Oswald - Midcontinent ISO, Inc. - 2	
Answer	No
Document Name	
Comment	
By adding control to the statement "Real-time monitoring" from TOP-003 and IRO-010 won't this set an expectation that control data will be part of those standards by default. The implementation guidance for CIP-012-1 in the identification of security protection section has taken out the wording of control so just in the documents providing guidance has contradictions of the Real-time monitoring of data. Recommendation that if control is to be part of "Real-time monitoring" then make the modifications across the board including in the Glossary. The way it is right now adds to the misunderstanding and different interruption that and entity could have in trying to create an implementation plan.	
Likes 0	
Dislikes 0	
Response	
Brandon McCormick - Brandon McCormick On Behalf of: Ginny Beigel, City of Vero Beach, 3; Lynne Mila, City of Clewiston, 4; Mike Blough, Kissimmee Utility Authority, 5, 3; Tom Reedy, Florida Municipal Power Pool, 6; - Brandon McCormick, Group Name FMPA	
Answer	No
Document Name	
Comment	

FMPA agrees with the following comments from Lakeland Electric:

NERC SDTs need to start revising language related to the number of regions with the removal of the SPP RE (p. 3).

General Considerations for Requirement R1: document should be documented plan

Alignment with IRO and TOP standards: last sentence “Real-time Monitoring “, the M should not be capitalized as it is not a NERC defined term.

Likes 0	
Dislikes 0	

Response

Dennis Sismaet - Northern California Power Agency - 6

Answer	No
Document Name	

Comment

See Response to Question 1.

Likes 0	
Dislikes 0	

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6

Answer	No
Document Name	

Comment

PacifiCorp supports MEC’s comments and adds the following: With reference to the Technical Rationale “Control Center Ownership”, the WECC Data Exchange/EMS Work Group (DEMSWG) worked with vendors to perform inter-operability testing and also train utilities in how to obtain and install certificates. Initially companies could not implement Secure ICCP on a UNIX server because the implementation required a SISCO stack and an Intel windows based server. Obtaining a new certificate would require 10 days and would expire in 1 year. This certificate expiration presented a problem of renewal in a timely manner and because of this many utilities were wanting expiration periods from 3 to 15 years. There was concern if a certificate expired during the night or weekend as to what would happen to the data transfer. Eventually the inability to guarantee a valid certificate at all times doomed the implementation of Secure ICCP.

Likes 0	
Dislikes 0	

Response

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	
Comment	
We support MRO NSRF comments.	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 5	
Answer	No
Document Name	
Comment	
Reclamation recommends the changes proposed in the response to Question 1 be implemented in the Technical Rationale for consistency. Reclamation also recommends correcting the grammar in “General Considerations for Requirement R1 from: “Requirement R1 focuses on implemented a document plan…” to: “Requirement R1 focuses on implementing a documented process…”	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Aaron Austin - AEP - 3	
Answer	Yes
Document Name	
Comment	
AEP requests the SDT consider including some statements in Technical Rationale to address the possibility that data requests made related to TOP-003 and/or IRO-010 include other data that is not Real-time Assessment data or Real-time monitoring data and how the Responsible Entity could exclude this other data from the security requirements.	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	Yes
Document Name	
Comment	
City Light supports SRP comments	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
See MRO NSRF comments.	
Likes 0	
Dislikes 0	
Response	

Shannon Fair - Colorado Springs Utilities - 1,3,5,6, Group Name Colorado Springs Utilities	
Answer	Yes
Document Name	
Comment	
CSU agrees with the Technical Rationale and Justification for CIP-012 provided by the SDT. However, CSU continues to maintain that an additional 12 months be considered for the plan implementation aspect of Requirement R1. PDF page 6, paragraph 3 of section title *Identification of Where Security Protection is Applied by the Responsible Entity* states "The SDT understands that in data exchanges between Control Centers, a single entity may not be responsible for both ends of the communication link." With the intent of the standard being to secure communications between Control Centers (including communication between two separate entities Control Centers), this will call for inter-entity cooperation to ensure both sides of link are secure. This is where the additional 12 months would be necessary, for coordination of efforts from both entities.	
Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
NV Energy does believe the need for this Standard is necessary, and the Rationale and Justification document provides a sufficient amount of information for the need, and protections to consider. The documents focus is not to provide detailed implementation methods, but just provide the “why” for the Standard and its Requirement.	
Likes 0	
Dislikes 0	
Response	
John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1	
Answer	Yes
Document Name	
Comment	
No Comment	
Likes 0	
Dislikes 0	

Response
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company
Answer	Yes
Document Name	
Comment
Yes, without additional comment.
Likes 0	
Dislikes 0	
Response
Warren Cross - ACES Power Marketing - 1,3,4,5 - MRO,WECC,Texas RE,SERC,SPP RE,RF
Answer	Yes
Document Name	
Comment
No comment.
Likes 0	
Dislikes 0	
Response
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion, NextEra and HQ
Answer	Yes
Document Name	
Comment
Recommend removing the diagram because it does not represent enough examples. We believe the scope is understandable without the diagram
Likes 0	
Dislikes 0	
Response

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	Yes
Document Name	
Comment	
The SPP Standards Review Group suggests revising language in the General Considerations for Requirement R1 to read as follows: Requirement R1 focuses on implementing a documented plan to protect information that is critical to the Real-time operations of the Bulk Electric System while in transit between applicable Control Centers.	
Likes 0	
Dislikes 0	
Response	

Russell Martin II - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
SRP agrees with the Technical Rationale and Justification for CIP-012 provided by the SDT. However, SRP continues to maintain that an additional 12 months be considered for the plan implementation aspect of Requirement R1. PDF page 6, paragraph 3 of section title *Identification of Where Security Protection is Applied by the Responsible Entity* states "The SDT understands that in data exchanges between Control Centers, a single entity may not be responsible for both ends of the communication link." With the intent of the standard being to secure communications between Control Centers (including communication between two separate entities Control Centers), this will call for inter-entity cooperation to ensure both sides of link are secure. This is where the additional 12 months would be necessary, for coordination of efforts from both entities.	
Likes 0	
Dislikes 0	
Response	

Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
When addressing the security protections, the rationale should include that logical and physical controls can be used. This should include the team’s rationale for allowing these alternatives.	
Likes 0	

Dislikes 0	
Response	
Kristine Ward - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
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	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Faz Kasraie - Seattle City Light - 5 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thomas Breene - WEC Energy Group, Inc. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1,3,5 - WECC	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Douglas Johnson - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 3, Group Name FirstEnergy Corporation	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrey Komissarov - Andrey Komissarov On Behalf of: Jerome Gobby, Sempra - San Diego Gas and Electric, 3, 5, 1; - Andrey Komissarov	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Russell Noble - Cowlitz County PUD - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Heather Morgan - EDP Renewables North America LLC - 5	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Jack Cashin - American Public Power Association - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jamie Prater - Entergy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF	
Answer	
Document Name	
Comment	
See the NSRF comments provided in the Implementation Guidance section.	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	
Document Name	
Comment	
Duke Energy suggests a clarifying addition to the diagram on page 3 (Control Centers in Scope) of the Technical Rationale and Justification document. In order to make the diagram more closely align to the statement made on page 8 of the Implementation Guidance which states: *"Entity Alpha does not need to consider any communications to other non-Control Center facilities such as generating plants or substations. These communications are out of scope for CIP-012-1."* The statement above indicates that communications from a Control Center, to a non-Control Center (generation or sub) are out of scope. We suggest that a dotted line be added to the diagram on page 3 (Control Centers in Scope) of the Technical Rational and Justification document to show that communications from a GOP Control Center to a GOP Control Room should be considered out of scope. It is possible that a scenario could exist where GOP Control Centers pass information through a GOP Control Room out to Field Assets.	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	
Document Name	
Comment	
AECI supports comments provided by NRECA	

Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE is concerned BCAs and EACMs used for CIP-012-1 may be considered out of scope for the rest of the CIP Reliability Standards based on a statement on Page 6: "*The SDT also recognizes that CIP-012 security protection may be applied to a Cyber Asset that is not an identified BES Cyber Asset or EACMS. The identification of the Cyber Asset as the location where security protection is applied does not expand the scope of Cyber Assets identified as applicable under the CIP Cyber Security Standards CIP-002 through CIP-011*." There appears to be a typo in the footer as it shows Reliability Standard CIP-002-1, instead of CIP-012-1.	
Likes 0	
Dislikes 0	
Response	

4. The SDT modified the draft Implementation Guidance for CIP-012 to provide examples of how a Responsible Entity could comply with the requirements. The draft Implementation Guidance does not prescribe the only approach to compliance. Rather, it describes what the SDT believes would be effective ways to comply with the standard. See NERC's Compliance Guidance policy for information on Implementation Guidance. Do you agree with the draft Implementation Guidance? If you do not agree, or if you agree but have comments or suggestions for the draft Implementation Guidance, please provide your recommendation and explanation.

Russell Martin II - Salt River Project - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

Overall, SRP does not agree with twenty-four (24) calendar months for the implementation of Requirements R1, as R1 and R2 from the second draft have been merged. Although SRP recognizes the SDT is not specifying the controls to be used to protect confidentiality and integrity, the only examples provided in the implementation guidance includes encryption. If there are other methods available to achieve the security objective, SRP asks the SDT to provide them. However, the only method available to achieve the proposed required objective, on the ICCP network, is to implement encryption. As FERC order 822 states on page 37, "if several registered entities have joint responsibility for a cryptographic key management system used between their respective Control Centers, they should have the prerogative to come to a consensus on which organization administers that particular key management system." Furthermore, the FERC order states on page 38, "While responsible entities are required to exchange real-time and operational planning data necessary to operate the bulk electric system using mutually agreeable security protocols, there is no technical specification for how this transfer of information should incorporate mandatory security controls." These are activities and specifications that must be created and agreed upon by all registered entities involved in the data

transfer. As such the timeline is reliant on registered entities working together on a common solution and would not be achievable within 24 calendar months.

Additionally, if encryption fails, SRP would lose Real-time Assessment and Real-time monitoring and control data. There are many opportunities for encryption to fail that must be addressed. The implementation of encryption requires a pilot to truly understand and address the mechanisms of failure, the impacts encryption would cause on the exchange of the data, and the computing resources required. A pilot also requires a great amount of coordination to execute, not only within the industry, but may also include carriers, vendors, and possibly third-party encryption key program managers.

Because of the aforementioned reasons and concerns, SRP is recommending a phased implementation for CIP-012-1. A 24 month implementation is appropriate, but only for Requirement R1. The 24 months for R1 would provide time to coordinate and create an industry-wide solution. SRP is proposing the SDT include an additional 12 months for the plan implementation aspect of Requirement R1. The additional 12 months would be used for a pilot and course correction if needed, in addition to understanding, formulating, and executing maintenance strategies.

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion, NextEra and HQ

Answer	No

Document Name	
Comment	
Request a definition of “logical protection” or replace all instances of “logical protection” with “encryption”	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 5	
Answer	No
Document Name	
Comment	
Reclamation recommends the term “plan” be replaced with the term “process” throughout the CIP-012-1 standard, Technical Rationale, Implementation Guidance, and associated documents. A plan is an unwarranted layer of compliance that does not improve the reliability of the BES. The processes an entity chooses to implement are what improve the reliability of the BES.	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	
Comment	
We support MRO NSRF comments. Additionally, The Implementation Guidance doesn’t address our comments to question 1. And, the Implementation Guidance starts with “as noted in the Technical Rationale.” Does this cross reference blur the lines between the two?	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No

Document Name	
Comment	
PacifiCorp supports MEC's comments.	
Likes 0	
Dislikes 0	
Response	
John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1	
Answer	No
Document Name	
Comment	
Implementation of R1.3 will require a standardized solution/technology between entities and a hierarchy of entity responsibilities. Recommend the SDT add guidance and a requirement to identify the entity who is the controlling authority for the secure communications between two or more entities.	
Likes 0	
Dislikes 0	
Response	
Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	
Comment	
See Response to Question 1.	
Likes 0	
Dislikes 0	
Response	
Brandon McCormick - Brandon McCormick On Behalf of: Ginny Beigel, City of Vero Beach, 3; Lynne Mila, City of Clewiston, 4; Mike Blough, Kissimmee Utility Authority, 5, 3; Tom Reedy, Florida Municipal Power Pool, 6; - Brandon McCormick, Group Name FMPA	
Answer	No
Document Name	

Comment
FMPA agrees with the following comments from Lakeland Electric: The draft Implementation Guidance document provides references to the TOP-003 and IRO-010 for the operating information/data that should be protected. It appears that there may be opportunities for differences in interpretation depending on what specifications are requested by the RC or the TOP per **IRO-010 R1**: "A list of data and information needed by the Reliability Coordinator to support its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments including non-BES data and external network data, as deemed necessary by the Reliability Coordinator. And, **TOP-003 R1 1.1.** A list of data and information needed by the Transmission Operator to support its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments including non-BES data and external network data as deemed necessary by the Transmission Operator." It seems that the list of items enumerated in the NERC Glossary definition for Real-time Assessment: "The assessment shall reflect applicable inputs including, but not limited to: load, generation output levels, known Protection System and Special Protection System status or degradation, Transmission outages, generator outages, Interchange, Facility Ratings, and identified phase angle and equipment limitations" should be the starting point instead of the R1 requirements referenced in the CIP-012. If an entity needed to add more, there should be some way of incorporating more, but the baseline should be the inputs listed in the RTA definition. Does an entity that is only participating in sharing information via the ICCP network and that does not need to send data to a backup control center (ie, a TOP operating out of a substation control house or a GOP that may operate two facilities) need to meet the same requirements as an entity with actual Control Center/Backup Control Center NERC obligations? It seems to me that the scope for the low impact Control Centers might be limited and reduced in scope.

Likes 0	
Dislikes 0	

Response

James Anderson - CMS Energy - Consumers Energy Company - 1	
Answer	No
Document Name	

Comment
To be consistent with other CIP standards, please combine Technical Rational and Justification document with the Implementation Guidance document and then incorporate the new document into the draft standard. Please clarify that CIP-012 is a standalone standard that is not associated with all the other CIP standards.

Likes 0	
Dislikes 0	

Response

Darnez Gresham - Darnez Gresham On Behalf of: Annette Johnston, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Darnez Gresham	
Answer	No
Document Name	

Comment	
We support MRO NSRF comments. Additionally, The Implementation Guidance doesn't address our comments to question 1. And, the Implementation Guidance starts with "as noted in the Technical Rationale." Does this cross reference blur the lines between the two?	
Likes 0	
Dislikes 0	
Response	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	No
Document Name	
Comment	
MMWEC supports comments submitted by NPCC.	
Likes 0	
Dislikes 0	
Response	
Marty Hostler - Northern California Power Agency - 5	
Answer	No
Document Name	
Comment	
See Response to Question 1.	
Likes 0	
Dislikes 0	
Response	
Shannon Fair - Colorado Springs Utilities - 1,3,5,6, Group Name Colorado Springs Utilities	
Answer	No
Document Name	
Comment	

Overall, CSU does not agree with twenty-four (24) calendar months for the implementation of Requirements R1, as R1 and R2 from the second draft have been merged. Although CSU recognizes the SDT is not specifying the controls to be used to protect confidentiality and integrity, the only examples provided in the implementation guidance includes encryption. If there are other methods available to achieve the security objective, CSU asks the SDT to provide them. However, the only method available to achieve the proposed required objective, on the ICCP network, is to implement encryption. As FERC order 822 states on page 37, “if several registered entities have joint responsibility for a cryptographic key management system used between their respective Control Centers, they should have the prerogative to come to a consensus on which organization administers that particular key management system.” Furthermore, the FERC order states on page 38, “While responsible entities are required to exchange real-time and operational planning data necessary to operate the bulk electric system using mutually agreeable security protocols, there is no technical specification for how this transfer of information should incorporate mandatory security controls.” These are activities and specifications that must be created and agreed upon by all registered entities involved in the data transfer. As such the timeline is reliant on registered entities working together on a common solution and would not be achievable within 24 calendar months.

Additionally, if encryption fails, CSU would lose Real-time Assessment and Real-time monitoring and control data. There are many opportunities for encryption to fail that must be addressed. The implementation of encryption requires a pilot to truly understand and address the mechanisms of failure, the impacts encryption would cause on the exchange of the data, and the computing resources required. A pilot also requires a great amount of coordination to execute, not only within the industry, but may also include carriers, vendors, and possibly third-party encryption key program managers.

Because of the aforementioned reasons and concerns, CSU is recommending a phased implementation for CIP-012-1. A 24 month implementation is appropriate, but only for Requirement R1. The 24 months for R1 would provide time to coordinate and create an industry-wide solution. CSU is proposing the SDT include an additional 12 months for the plan implementation aspect of Requirement R1. The additional 12 months would be used for a pilot and course correction if needed, in addition to understanding, formulating, and executing maintenance strategies.

Likes 0	
Dislikes 0	

Response

Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body

Answer	No
Document Name	

Comment

City Light supports SRP comments

Likes 0	
Dislikes 0	

Response

Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,4,5 - RF

Answer	No
Document Name	

Comment

To be consistent with other CIP standards, please combine Technical Rational and Justification document with the Implementation Guidance document and then incorporate the new document into the draft standard. Please clarify that CIP-012 is a standalone standard that is not associated with all the other CIP standards.

Likes 0	
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion

Answer	No
Document Name	

Comment

On page 5 under section “Identification of Where Security Protection is Applied by the Responsible Entity”, language should be added to address the situation where a Responsible Entity does not manage either end of a communication link, indicating that this Responsible Entity does not have compliance obligations to R1.2.

Likes 0	
Dislikes 0	

Response

Patricia Lynch - NRG - NRG Energy, Inc. - 5,6

Answer	No
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2

Answer	Yes
Document Name	

Comment

When addressing the security protections that can be used in meeting CIP-012, examples of physical protection should be included in guidance. This should include details on how they can be used to address various parts of the communication between Control Centers. {C}

Likes 0	
Dislikes 0	

Response

Warren Cross - ACES Power Marketing - 1,3,4,5 - MRO,WECC,Texas RE,SERC,SPP RE,RF

Answer	Yes
Document Name	

Comment

Yes. For the requirement to be less prescriptive, additional technical and implementation guidance is needed to provide clarity on the SDT intent and audited scope.

Likes 0	
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	Yes
Document Name	

Comment

Yes, without additional comment.

Likes 0	
Dislikes 0	

Response

Jack Cashin - American Public Power Association - 4

Answer	Yes
Document Name	

Comment

no comment	
Likes 0	
Dislikes 0	
Response	
Ellen Oswald - Midcontinent ISO, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Currently it is good guidance document but until an entity does actual implementation and experiences any issues that arise from the implementation of CIP-012 requirement one can only assume the outcome.	
Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
NV Energy believes the document is necessary for CIP-012-1, due to its complexity. The document still requires additional clarity on protections associated with data protection on ICCP communication. The document reflects a lack of research into current technology availability, feasibility, and costs for this common type of Control Center communication.	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1	
Answer	Yes
Document Name	
Comment	

Suggestion for last paragraph under **Identification of Where Security Protection is Applied by the Responsible Entity.** Split into two separate paragraphs. One describing how to handle “when exchanging data between two entities” and another focused on “when a Responsible Entity owns and operates both Control Centers.”

Likes 0	
Dislikes 0	

Response

Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman

Answer	Yes
Document Name	

Comment

See MRO NSRF comments.

Likes 0	
Dislikes 0	

Response

Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF

Answer	Yes
Document Name	

Comment

The NSRF would like to thank the drafting team for their guidance and especially under the Reference Model and Reference Model discussion within the Implementation Guidance document. Since the Requirement within this Standard is purposely non-prescriptive due to the various operating conditions for which security can be applied it is important to have model applications for entities to apply the Standard to their particular operations and in a consistent manner among the industry.

The NSRF notes that the drafting team stated in their previous draft response that they will submit the Implementation Guidance for ERO endorsement, thank you. However, the NSRF notes that the current “Technical Rationale for Reliability Standards” initiative underway may alter how “Compliance Guidance” during the drafting/balloting process is handled. The Reference Model section of CIP-012 is a good example of providing drafting team application and intent that is essential to the understanding of a Standard. Although the preferred approach would be to have Implementation Guidance issued prior to a Standards’ effective date, we would hope that when moving forward with the “Technical Rationale for Reliability Standards Initiative” that in cases, such as mentioned with the CIP-012, that these types of sections would be included within the Technical Rationale section or by another means for clarification of Standard application.

Likes 0	

Dislikes 0	
Response	
Aaron Austin - AEP - 3	
Answer	Yes
Document Name	
Comment	
AEP requests the SDT consider including some statements in Implementation Guidance to address the possibility that data requests made related to TOP-003 and/or IRO-010 include other data that is not Real-time Assessment data or Real-time monitoring data and how the Responsible Entity could exclude this other data from the security requirements.	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jamie Prater - Entergy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Heather Morgan - EDP Renewables North America LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Russell Noble - Cowlitz County PUD - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrey Komissarov - Andrey Komissarov On Behalf of: Jerome Gobby, Sempra - San Diego Gas and Electric, 3, 5, 1; - Andrey Komissarov	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 3, Group Name FirstEnergy Corporation	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Douglas Johnson - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1,3,5 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thomas Breene - WEC Energy Group, Inc. - 3	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Faz Kasraie - Seattle City Light - 5 - WECC	
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	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kristine Ward - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE is not comfortable commenting on Implementation Guidance until the standard language is in its final form.	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	
Document Name	
Comment	

AECI supports comments provided by NRECA	
Likes 0	
Dislikes 0	
Response	

5. The SDT believes proposed CIP-012-1 provides entities with flexibility to meet the reliability objectives in a cost effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost effective approaches, please provide your recommendation and, if appropriate, technical justification.

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion

Answer	No
Document Name	

Comment

While the standard is flexible on methodology, the requirement to coordinate with the other Responsible Entity may limit the inherent flexibility by requiring one Responsible Entity to make Capital Investments to meet the security requirements of the other Responsible Entity.

Likes 0	
Dislikes 0	

Response

Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,4,5 - RF

Answer	No
Document Name	

Comment

More flexibility and less guidance could lead to inconsistency on requirement implementation among different entities.

Likes 0	
Dislikes 0	

Response

Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body

Answer	No
Document Name	

Comment

City Light supports SRP comments

Likes 0	
Dislikes 0	

Response

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	

BPA believes that if the data must be protected throughout the transmission, it would seem that could only be accomplished with encryption. For cases where the existing equipment is not capable of encryption, replacement will be costly and implementation lengthy.

Due to BPA's large amount of applicable data, access to funds and budget cycle, and resources to perform work required, the solution will be costly.

Likes 0	
Dislikes 0	

Response

Shannon Fair - Colorado Springs Utilities - 1,3,5,6, Group Name Colorado Springs Utilities	
Answer	No
Document Name	
Comment	

CSU does not agree the current standard and implementation plan can be executed in a cost effective manner. Encryption has been the only presented solution provided by auditors and SDT guidance to protect both confidentiality and integrity for the data within this scope. If the implementation timeframe remains at 24 months, more resources and capital will be required versus a phased implementation. A phased implementation provides the ability to not only ensure the most effective plan, but also provides the ability to plan more accurately within budget cycles. More importantly, if encryption fails, CSU would lose Real-time Assessment and Real-time monitoring and control data. CSU is concerned a 24 month implementation timeline would impact reliability as there are many opportunities for encryption to fail that must be addressed. This has a direct correlation on cost when addressing those opportunities during this timeframe.

Additionally, CSU would like to see reference models of methods that do not require encryption as a method to protect communications between Control Centers.

Likes 0	
Dislikes 0	

Response

Marty Hostler - Northern California Power Agency - 5	
Answer	No
Document Name	

Comment	
See Response to Question 1.	
Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Darnez Gresham On Behalf of: Annette Johnston, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Darnez Gresham	
Answer	No
Document Name	
Comment	
Without clarity on ICCP between Control Centers we cannot be certain of what is expected, the costs or flexibility.	
Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	
Comment	
Without additional expectations of ICCP communication protections, NV Energy is unable to determine the overall costs of CIP-012-1 implementation.	
Likes 0	
Dislikes 0	
Response	
James Anderson - CMS Energy - Consumers Energy Company - 1	
Answer	No
Document Name	
Comment	

More flexibility and less guidance could lead to inconsistency on requirement implementation among different entities.

Likes 0	
Dislikes 0	

Response

Brandon McCormick - Brandon McCormick On Behalf of: Ginny Beigel, City of Vero Beach, 3; Lynne Mila, City of Clewiston, 4; Mike Blough, Kissimmee Utility Authority, 5, 3; Tom Reedy, Florida Municipal Power Pool, 6; - Brandon McCormick, Group Name FMPA

Answer	No
Document Name	

Comment

FMPA agrees with the following comments from Lakeland Electric:

Depending on the outcome of the new definition of Control Center, there may be unintended consequences on the implementation of CIP-012 for small entities who only have BES Assets containing low impact BES Cyber Systems (i.e., Control Centers) --especially with the consideration of non-BES data and external network data. Industry is strongly motivated to protect the “right things” and maintain the BES so that it can continue to operate reliably, safely, and securely. Industry would be wise to carefully consider expansion of scope beyond what is truly required to protect the BES/critical infrastructure.

Likes 0	
Dislikes 0	

Response

Dennis Sismaet - Northern California Power Agency - 6

Answer	No
Document Name	

Comment

See Response to Question 1.

Likes 0	
Dislikes 0	

Response

Russell Noble - Cowlitz County PUD - 3

Answer	No

Document Name	
Comment	
Cowlitz PUD supports the comments submitted by the Bonneville Power Administration.	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
In the absence of clarity where ICCP is used for Real-time Assessment and Real-time monitoring data being transmitted between any Control Centers owned or operated by different Responsible Entities PacifiCorp cannot be certain of what is expected, regarding the costs or flexibility.	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	
Comment	
Without clarity on ICCP between Control Centers we cannot be certain of what is expected, the costs or flexibility.	
Likes 0	
Dislikes 0	
Response	
Warren Cross - ACES Power Marketing - 1,3,4,5 - MRO,WECC,Texas RE,SERC,SPP RE,RF	
Answer	No

Document Name	
Comment	
Cost effective manner as compared to what? Additional resources will be required and those resources will be needed to monitored 24x7 for those controls to be effective. I would think most entities would budget that as a considerable expense.	
Likes 0	
Dislikes 0	
Response	
Russell Martin II - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
SRP does not agree the current standard and implementation plan can be executed in a cost effective manner. Encryption has been the only presented solution provided by auditors and SDT guidance to protect both confidentiality and integrity for the data within this scope. If the implementation timeframe remains at 24 months, more resources and capital will be required versus a phased implementation. A phased implementation provides the ability to not only ensure the most effective plan, but also provides the ability to plan more accurately within budget cycles. More importantly, if encryption fails, SRP would lose Real-time Assessment and Real-time monitoring and control data. SRP is concerned a 24 month implementation timeline would impact reliability as there are many opportunities for encryption to fail that must be addressed. This has a direct correlation on cost when addressing those opportunities during this timeframe. Additionally, SRP would like to see reference models of methods that do not require encryption as a method to protect communications between Control Centers	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response

Kristine Ward - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	Yes
Document Name	
Comment	

what is cost effective to some, may not be cost effective to others. How do you define cost effective?

Additional Comments

If we identify multiple types of security protection for R1.1, and one of the forms of protection fails for whatever reason, however, Seminole believes we are still “protecting” the data transmission to the intent of the Standard via our other form(s) of protection, how is the drafting team addressing this?

Likes 0	
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	

Yes, without additional comment.

Likes 0	
Dislikes 0	

Response

Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino	
Answer	Yes
Document Name	
Comment	

Likes 0	

Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
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	
Faz Kasraie - Seattle City Light - 5 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thomas Breene - WEC Energy Group, Inc. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1,3,5 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Douglas Johnson - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 3, Group Name FirstEnergy Corporation	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Ellen Oswald - Midcontinent ISO, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Andrey Komissarov - Andrey Komissarov On Behalf of: Jerome Gobby, Sempra - San Diego Gas and Electric, 3, 5, 1; - Andrey Komissarov	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Heather Morgan - EDP Renewables North America LLC - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion, NextEra and HQ	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jamie Prater - Entergy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Austin - AEP - 3	
Answer	
Document Name	
Comment	
No Comment	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	
Document Name	
Comment	

AECI supports comments provided by NRECA	
Likes 0	
Dislikes 0	
Response	
John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1	
Answer	
Document Name	
Comment	
No Comment	
Likes 0	
Dislikes 0	
Response	
Jack Cashin - American Public Power Association - 4	
Answer	
Document Name	
Comment	
no comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE does not have comments on this question.	

Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	
Document Name	
Comment	
No answer or comments.	
Likes 0	
Dislikes 0	
Response	

Comments Received from Kara White at NRG Energy, Inc.

Questions

1. Requirement R1: The SDT drafted CIP-012-1 Requirement R1 for the Responsible Entity to implement one or more documented plan(s) to mitigate the risk of the unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring data while being transmitted between any Control Centers. Do you agree with this revision? If not, please provide the basis for your disagreement and an alternate proposal.

   ☐ Yes
   ☒ No

   Comments:

   NRG agrees with the revisions if they are a part of CIP-005, because: NRG thinks removing the term "control" could cause some misinterpretation within the industry, this change could also broaden the scope of what protocols are included in standard. NRG recommends that the security protections described in CIP-012 R1 go from EAP (Electronic Access Point) to EAP. This would eliminate the risk of a compromise of the data due to an attack on a Responsible Entities' corporate network (outside the ESP).

   NRG recommends that the scope of R1 of CIP-012 be added instead directly into CIP-005 and CIP-003 as additional requirements (instead of a separate requirement in a CIP-012 standard).

2. Implementation Plan: The SDT established the Implementation Plan to make the standard effective the first day of the first calendar quarter that is twenty-four (24) calendar months after the effective date of the applicable governmental authority's order approving the standard, or as otherwise

provided for by the applicable governmental authority. Do you agree with this proposal? If you think an alternate implementation time period is needed, please provide a detailed explanation of actions and time needed to meet the implementation deadline.

☒ Yes
☐ No

Comments:

3. The SDT modified the draft Technical Rationale and Justification for CIP-012 to assist in understanding the technology and technical requirements in the Reliability Standard. It also contains information on the SDT's intent in drafting the requirements. Do you agree with the technology and technical requirements in the draft Technical Rationale and Justification? If you do not agree, or if you agree but have comments or suggestions for the draft Technical Rationale and Justification, please provide your recommendation and explanation.

☐ Yes
☒ No

Comments: NRG recommends that NERC SDT see NRG comments for CIP-012 R1 relating to inclusion of EAP to EAP for protections scope.

4. The SDT modified the draft Implementation Guidance for CIP-012 to provide examples of how a Responsible Entity could comply with the requirements. The draft Implementation Guidance does not prescribe the only approach to compliance. Rather, it describes what the SDT believes would be effective ways to comply with the standard. See NERC's Compliance Guidance policy for information on Implementation Guidance. Do you agree with the draft Implementation Guidance? If you do not agree, or if you agree but have comments or suggestions for the draft Implementation Guidance, please provide your recommendation and explanation.

☐ Yes
☒ No

Comments: NRG requests that NERC SDT see comments above. There are more prescriptive inclusion of protocols in other requirements and therefore, NRG thinks that this proposed standard as written may cause confusion within industry regarding implementation scope.

5. The SDT believes proposed CIP-012-1 provides entities with flexibility to meet the reliability objectives in a cost effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost effective approaches, please provide your recommendation and, if appropriate, technical justification.

☐ Yes
☒ No

Comments: NRG asserts that the vague nature of the requirement does not meet the reliability objective in a cost effective manner, because it does not specify the protocols in the requirement; therefore, the industry could misinterperet the scope of the requirement

Comments received from Laura McLeod at NB Power Corporation

Questions

1. Requirement R1: The SDT drafted CIP-012-1 Requirement R1 for the Responsible Entity to implement one or more documented plan(s) to mitigate the risk of the unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring data while being transmitted between any Control Centers. Do you agree with this revision? If not, please provide the basis for your disagreement and an alternate proposal.

   ☐ Yes
   x☐ No

   Comments: 1) The applicability of this requirement is uncertain given the proposed Control Center definition has not been approved. 2) R1 also notes that oral communications is excluded. Why not clarify that email is also excluded given the last paragraph page 8 of the implementation guidance.

2. Implementation Plan: The SDT established the Implementation Plan to make the standard effective the first day of the first calendar quarter that is twenty-four (24) calendar months after the effective date of the applicable governmental authority's order approving the standard, or as otherwise provided for by the applicable governmental authority. Do you agree with this proposal? If you think an alternate implementation time period is needed, please provide a detailed explanation of actions and time needed to meet the implementation deadline.

   x☐ Yes
   ☐ No

   Comments:

3. The SDT modified the draft Technical Rationale and Justification for CIP-012 to assist in understanding the technology and technical requirements in the Reliability Standard. It also contains information on the SDT's intent in drafting the requirements. Do you agree with the technology and technical requirements in the draft Technical Rationale and Justification? If you do not agree, or if you agree but have comments or suggestions for the draft Technical Rationale and Justification, please provide your recommendation and explanation.

   x☐ Yes
   ☐ No

   Comments: References to the specifications required under TOP-003 and IRO-010 should specifically state that data necessary to perform operational planning analysis is not applicable if not used for real time assessments.

4. The SDT modified the draft Implementation Guidance for CIP-012 to provide examples of how a Responsible Entity could comply with the requirements. The draft Implementation Guidance does not prescribe the only approach to compliance. Rather, it describes what the SDT believes would be effective ways to comply with the standard. See NERC's Compliance Guidance policy for information on Implementation Guidance. Do you agree with the draft Implementation Guidance? If you do not agree, or if you agree but have comments or suggestions for the draft Implementation Guidance, please provide your recommendation and explanation.

x☐ Yes
☐ No

Comments:

5. The SDT believes proposed CIP-012-1 provides entities with flexibility to meet the reliability objectives in a cost effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost effective approaches, please provide your recommendation and, if appropriate, technical justification.

☐ Yes
x☐ No

Comments: An entities State Estimator can identify (and ignore) off normal values. This inherent capability reduces the risk that flawed or incorrect data will be utilized in real time assessments.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP-012-1

Project 2016-02 Modifications to the CIP Standards: Consideration of Comments

May 2018

RELIABILITY | ACCOUNTABILITY



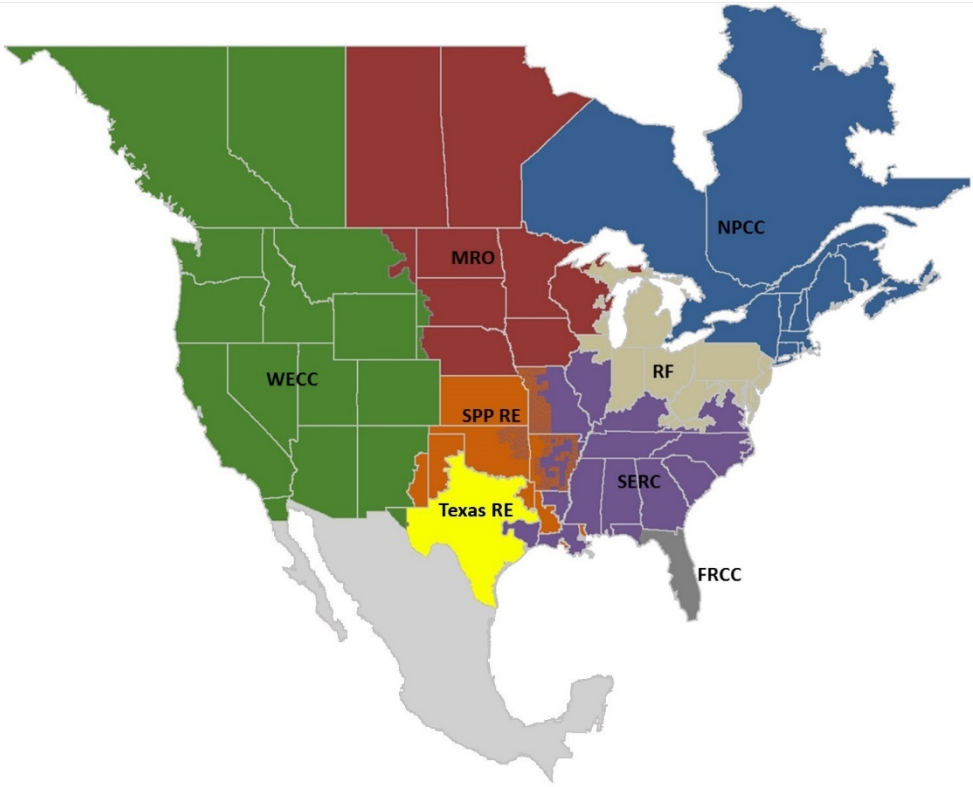

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Preface

The vision for the Electric Reliability Organization (ERO) Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the eight Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

The North American BPS is divided into eight RE boundaries as shown in the map and corresponding table below.



The North American BPS is divided into eight RE boundaries. The highlighted areas denote overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.

FRCC	Florida Reliability Coordinating Council
MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
SPP RE	Southwest Power Pool Regional Entity
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

Background

The Project 2016-02 Modifications to CIP Standards Drafting Team thanks all commenters who submitted comments on the draft CIP-012-1 standard. This standard was posted for a 45-day public comment period through Friday, April 30, 2018. Stakeholders were asked to provide feedback on the standards and associated documents through a special electronic comment form. There were 58 sets of responses, including comments from approximately 155 different people from approximately 108 companies representing the 10 Industry Segments as shown in the table on the following pages.

All comments submitted may be reviewed in their original format on the standard's project page.

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process. If you feel there has been an error or omission, you can contact the NERC standards developer, Jordan Mallory, at 404-446-2589 or at jordan.mallory@nerc.net.

CIP-012-1 Consideration of Comments

Purpose

The Modification to CIP Standards drafting team appreciates industry's comments on the CIP-012-1 standard. The CIP standards drafting team (SDT) thanks everyone for their comments. The SDT reviewed all comments carefully and made changes to the standard accordingly. The following pages are a summary of the comments received and how the CIP SDT addressed them. If a specific comment was not addressed in the summary of comments, please contact the NERC standards developer.

Control Center Definition

Many commenters expressed concern with the proposed Control Center definition.

The SDT thanks everyone for their comments. The SDT decided to draft exemption language within the applicability section of CIP-012 instead of revising the Control Center definition. Please see the Control Center definition consideration of comments report for additional SDT responses on the new path taken by the SDT.

Requirement R1

A commenter expressed that Real-time Assessments list a number of specific inputs that should be considered for both "Real-time Assessment (RTA) and Real-time monitoring (RTm) data." The commenter suggested there may be an audit approach taken that would require consideration of both RTA AND RTm data for proof that an entity provided adequate protections. The commenter requested that the SDT provide clarification on whether there is a distinction between data used for the RTA and data used for RTm. The commenter recommended consideration of the use of the inputs in the RTA NERC term with a caveat that Entities may choose to protect additional data if they feel the need to expand the scope.

The TOP-003-3 Requirement R1 already requires TOPs identify data used for RTA and RTm.

Some commenters questioned if CIP Exceptional Circumstance language needed to be added CIP-012-1.

The CIP Exceptional Circumstance language has been added to CIP-012.

A commenter expressed that "security protection used to mitigate risk" is too ambiguous. The commenter requested the SDT consider including two concepts in Requirement R1. The first concept is to clarify whether currently in place ICCP should be encrypted. The commenter noted that the requirement states "while being transmitted between any Control Centers." The commenter further noted that the draft Implementation Guidance has content talking about "both ends of the link" but did not include the expectations for the data while on the link. The commenter was concerned with latency (primarily for generation control) if secure encryption is expected over the ICCP. Second concept is to include examples that include but are not limiting for security protection.

The SDT asserts that defining a plan to mitigate the risk of modification and disclosure of applicable data allows the Responsible Entity to document the processes that are supportable within its organization and offers flexibility in methods to meet the security objective. The SDT notes that the Implementation Guidance document offers examples of how to comply with the standard.

The SDT encourages Responsible Entities to submit additional scenarios as Implementation Guidance[1] through pre-qualified organizations for endorsement consideration.

[1] NERC Compliance Guidance Policy: https://www.nerc.com/pa/comp/guidance/Documents/Pre-qualified_org_submittal_with_form.pdf

Some commenters expressed that CIP-012 is unnecessary and that IRO-010 and TOP-003 already require a mutually agreeable security protocol. Additionally, another commenter expressed concern about the overlap between CIP-012 and TOP-003-3/IRO-010-2. The commenter questioned whether these standards should be combined.

The SDT asserts that the standard is necessary to protect the confidentiality and integrity of applicable data transmitted between Control Centers and is responsive to the directive in Order No. 822.

A commenter requested clarity on the Responsible Entity in charge of securing the data being transmitted from a generator on RC, BA, and TOP equipment. The commenter suggested that the RC, BA, and TOP identify the GOP responsibilities under Part 1.3.

If the Generator is not a Control Center then CIP-012 does not apply as it is only between Control Centers. However, if the Generator is an applicable Control Center, then Requirement R1 Part 1.3 is intended to require the entities to document their responsibilities.

A commenter requested the SDT clarify whether CIP-012-1 applies to low, medium, or high BES Cyber Systems. The commenter requested the SDT also consider how to incorporate the scoping criteria into CIP-002.

The SDT asserts that the applicability is clear. It applies to in-scope data being transmitted between Control Centers as defined in the NERC Glossary of Terms and is applicable to all impact levels.

Some commenters noted that Real-time monitoring is not a defined term and that the R in Real-time should not be capitalized. In addition, the commenters expressed concern that coordination between Control Centers may result in compromises that may not satisfy the needs of the entities involved.

The term "Monitor" has been lowercased. “Real-time" is defined in the NERC Glossary of Terms and correctly used.

A commenter expressed concern that Operations Planning Analysis (OPA) data is not included in CIP-012-1. In addition, the commenter also noticed the Violation Time Horizon is for Operations Planning. Since the SDT has indicated reasons for excluding OPA data, the commenter asked whether the relevant Violation Time Horizon should be Real-time Operation.

Please see CIP-012-1 Consideration of Comments Summary Response for the OPA part. Due to the plan being drafted ahead of time; it would not be considered a Real-time Horizon and should remain operations planning horizon.

A commenter disagreed that having a plan adds to the reliability of protecting data used for Real-time Assessment and Real-time monitoring and commented that a plan is not needed. Some commenters recommended replacing the term “plan” with “process” throughout CIP-012-1, the Technical Rationale, Implementation Guidance, and other associated documents. Additionally, some commenters recommended that entities not be required to have a plan in Requirement R1, but have an actionable Requirement to implement. A suggestion was provided.

Based on industry feedback from a prior comment period, the SDT chose a requirement structure that is consistent with many other CIP standards to implement a documented plan. With regard to the use of the “process” instead of "plan", the SDT notes that the term ‘documented process’ refers to a set of required instructions specific to the Responsible Entity, designed to achieve a specific outcome. The plan to meet R1 may simply include documentation of the required elements of the Parts of CIP-012-1 Requirement R1. The plan also allows for R1 Part 1.3 to document the entities’ responsibilities.

A commenter asked whether the current set of standards address those additional vulnerabilities in the entity’s IT Security Plan. The commenter suggested that the current plan should be updated to include these additional risks, threats and integrated solution(s) that are already performed by the entity.

The documented plan(s) will need to address the security protection in place to mitigate the risk of unauthorized disclosure or modification of applicable data transmitted between any Control Centers in accordance with the specified attributes in the Requirement Parts.

Implementation Plan

Some commenters stated that the 24-month timeline is not enough and requested the implementation timeline be increased to 36 months or a phased-in approach. Additionally, a commenter acknowledged that the standard and implementation plan are silent on physical security for the equipment being used to provide the data protection. The commenter provided an example of protection for a router that is located in another Entity's facility.

The SDT carefully considered all comments and concluded that many factors should be considered to determine an implementation period. These factors include complexity of technology solutions, quantity of telecommunications lines requiring controls and coordination with other Responsible Entities/solution providers, among others. The SDT concluded that a twenty-four (24) month implementation period is appropriate.

Some commenters noted the difficulty on providing responses to the implementation timeline until the Control Center definition is developed.

Please see the Consideration of Comments for the Control Center definition for additional information on the SDT's approach.

Technical Rationale for CIP-012-1

Some entities requested the SDT consider including some statements in Technical Rationale to address the possibility that data requests made related to TOP-003 and/or IRO-010 include other data that is not Real-time Assessment data or Real-time monitoring data and how the Responsible Entity could exclude this other data from the security requirements.

The SDT asserts that it is up to the Responsible entity to ensure all RTA and RTm data that is transmitted between Control Centers is protected regardless of whether additional data is also exchanged in regards to the Technical Rationale and the Implementation Guidance Documents.

A commenter noted that when addressing the security protections, the rationale should include that logical and physical controls can be used. The commenter suggested this should include the team's rationale for allowing these alternatives.

The SDT asserts that the Technical Rationale document already specifies that logical or physical controls can be used to achieve the required security objective.

A commenter noted that the number of regions needs to be updated.

NERC will make appropriate revisions to various documents upon the effective date of the SPP RE dissolution.

Some commenters noted grammatical modifications:

- **In requirement R1 of the technical rationale document, the document should state document plan**
- **The alignment with IRO and TOP standards: last sentence "Real-time Monitoring ", the M should not be capitalized as it is not a NERC defined term.**

- **There appears to be a typo in the footer as it shows Reliability Standard CIP-002-1, instead of CIP-012-1**

The SDT agrees and will make the modification as noted.

A commenter suggested a clarifying addition to the diagram on page 3 (Control Centers in Scope) of the Technical Rationale document: "In order to make the diagram more closely align to the statement made on page 8 of the Implementation Guidance which states:

'Entity Alpha does not need to consider any communications to other non-Control Center facilities such as generating plants or substations. These communications are out of scope for CIP-012-1.'

The statement above indicates that communications from a Control Center, to a non-Control Center (generation or sub) are out of scope. We suggest that a dotted line be added to the diagram on page 3 (Control Centers in Scope) of the Technical Rational and Justification document to show that communications from a GOP Control Center to a GOP Control Room should be considered out of scope. It is possible that a scenario could exist where GOP Control Centers pass information through a GOP Control Room out to Field Assets."

The SDT asserts that the diagram clearly shows the communications that are in and out of scope. Additionally, this diagram is simply one example and is not inclusive of all possible communication scenarios.

A commenter noted that adding control to the statement "Real-time monitoring" from TOP-003 and IRO-010 may set an expectation that control data will be part of those standards by default. The commenter noted that the proposed CIP-012-1 Implementation Guidance does not use "and control." The commenter recommended that if control is to be part of "Real-time monitoring" then the SDT should make the modifications to all documents, including the Glossary, to reduce misunderstanding.

Based on comments from the prior ballot and comment period, the SDT removed "and control" from the requirement for this posting. The SDT notes that the systems that provide control are generally the same systems that provide monitoring. The SDT removed "and control" to be consistent with the TOP-003 and IRO-010 standards.

A commenter requested that the SDT be consistent with other CIP standards and suggested the SDT combine the Technical Rationale document with the Implementation Guidance document within the draft standard. The commenter also requested the SDT clarify that CIP-012 is a standalone standard that is not associated with all the other CIP standards.

The Technical Rationale document and Implementation Guidance document serve two different purposes. The Technical Rationale document provides the SDT's intent and technical basis for the language in the standard. In addition, the Technical Rationale document provides examples and diagrams to assist entities in understanding the language of the standard. Implementation Guidance is a means for registered entities to develop examples or approaches for ERO Enterprise endorsement to illustrate how registered entities could comply with a standard[2]. There is a project underway reviewing all of the current Technical Rationale documents and removing compliance examples from each document to submit for ERO Enterprise endorsement. Therefore, the Technical Rationale document and Implementation Guidance document cannot be merged together. While the applicability is different from other CIP standards, the CIP-012-1 is one standard within the CIP Standard family.

A commenter expressed concern regarding the BCAs and EACMS used for CIP-012-1 may be considered out of scope for the rest of the CIP Reliability Standards based on a statement on Page 6: "The SDT also recognizes that CIP-012 security protection may be applied to a Cyber Asset that is not an identified BES Cyber Asset or EACMS. The

[2] NERC Compliance Guidance Policy: https://www.nerc.com/pa/comp/guidance/Documents/Pre-qualified_org_submittal_with_form.pdf

identification of the Cyber Asset as the location where security protection is applied does not expand the scope of Cyber Assets identified as applicable under the CIP Cyber Security Standards CIP-002 through CIP-011."

The SDT notes that the assets where the security protection is applied under CIP-012 may not be part of an entity's identified BCAs or EACMS. If the asset meets the definition of a BCA or EACMS, it should be categorized as such. CIP-012-1 neither expands nor diminishes the scope of applicable Cyber Assets under CIP-002 through CIP-011.

Some commenters noted difficulty with implementing Secure ICCP in the past because of concerns over the inability to guarantee a valid certificate at all times.

The SDT asserts that implementation is not limited to Secure ICCP. Entities are allowed the implementation of physical or logical controls that best meet their operational and reliability needs as long as it meets the security objective specified in CIP-012-1 Requirement R1. This includes the management of certificates.

Implementation Guidance

A commenter mentioned that when addressing the security protection that can be used in meeting CIP-012, examples of physical protection should be included in guidance. This should include details on how they can be used to address various parts of the communication between Control Centers.

The SDT has addressed an example within the implementation guidance document that includes physical protections.

A commenter suggested that the last paragraph under Identification of where security protection is applied by the Responsible Entity be split into two separate paragraphs. The commenter suggested the first paragraph would describe how to handle "when exchanging data between two entities" and the second paragraph would focus on "when a Responsible Entity owns and operates both Control Centers."

The SDT agrees with the comment and split the paragraph into two separate paragraphs.

A commenter mentioned that the guidance document is good but until an entity does actual implementation and experiences any issues that arise from the implementation of CIP-012 requirement one can only assume the outcome.

The SDT notes there are a number of ways to demonstrate compliance with the requirement and encourages entities to develop and submit additional examples of Implementation Guidance through pre-qualified organizations for endorsement consideration.

A commenter stated that the implementation of R1.3 will require a standardized solution/technology between entities and a hierarchy of entity responsibilities. The commenter recommended the SDT add guidance and a requirement to identify the entity who is the controlling authority for the secure communications between two or more entities.

The SDT agrees that there will be coordination necessary to meet R1.3. The requirement has been written to allow flexibility on how entities work together on this requirement. The SDT notes there are a number of ways to demonstrate compliance with the requirement and encourages entities to develop and submit additional examples of Implementation Guidance through a pre-qualified organization for endorsement consideration.

Some commenters requested that the SDT define "logical protection" or replace all instances of "logical protection" with "encryption."

The SDT contends that the standard is written to not specify a particular technology. This allows the requirement to be flexible in encompassing future protection solutions.

Some commenters recognized the SDT is not specifying the controls to be used to protect confidentiality and integrity and that the only examples provided in the implementation guidance include encryption. The commenters requested that the SDT provide other methods available to achieve the security objective if they exist. The commenters suggested the commenter cited activities and specifications in FERC Order No. 822, such as key management between separate Responsible Entities, that must be created and agreed upon by all registered entities involved in the data transfer. The commenter suggested such activities may not be achievable in the 24-month implementation period.

The commenter also noted that a Responsible Entity would lose Real-time Assessment and Real-time monitoring and control data if encryption failed. The commenter suggested a pilot to implement encryption.

The SDT agrees that there will be coordination necessary to meet R1.3. The requirement has been written to allow flexibility on how entities work together on this requirement. The SDT notes there are a number of ways to demonstrate compliance with the requirement and encourages entities to develop and submit additional examples of Implementation Guidance through pre-qualified organizations for endorsement consideration.

A commenter identified that on page 5 under section "Identification of Where Security Protection is applied by the Responsible Entity", language should be added to address the situation where a Responsible Entity does not manage either end of a communication link, indicating that this Responsible Entity does not have compliance obligations to R1.2.

The SDT notes that the entities communicating the in-scope data are required to have a plan. The plan should specify the responsibilities of the Responsible Entities in protecting the applicable data.

A couple of comments were received that the requirement should be less prescriptive, and additional technical and implementation guidance is needed to provide clarity on the SDT intent and audited scope.

The SDT notes there are a number of ways to demonstrate compliance with the requirement and encourages entities to develop and submit additional examples of Implementation Guidance through pre-qualified organizations for endorsement consideration.

Cost Effectiveness

A commenter expressed concern that if the data must be protected throughout the transmission, it would seem that could only be accomplished with encryption. The commenter noted that are cases where the existing equipment is not capable of encryption, replacement will be costly and implementation lengthy. In addition, the commenter stated that due to the large amount of applicable data, access to funds and budget cycle, and resources to perform work required, the solution will be costly.

The 24-month implementation timeline is to allow for selection the most practical solution, as well as for budgeting and acquisition and implementation.

Some commenters noted that without clarity on ICCP between Control Centers, the commenters cannot be certain of what is expected, the costs or flexibility.

The SDT notes that data in scope may not be limited to ICCP. This is dependent on the specifics of each entity or entities.

A commenter acknowledged that more flexibility and less guidance could lead to inconsistency on requirement implementation among different entities.

CIP-012 is written to allow for selection of the most practical solution for the entity or entities.

A commenter expressed that what is cost effective to some, may not be cost effective to others and questioned the definition of cost effectiveness.

CIP-012 is written to allow for selection of the most practical solution for the entity or entities.

A commenter questioned how the SDT is addressing the scenario where a Responsible Entity identifies multiple types of security protection and one of the forms fails but the data transmission is still protected, meeting the intent of the standard.

In the event of a failure of a protection method, it is the Entity's responsibility to demonstrate how compliance was maintained during the event.

A commenter does not agree the current standard and implementation plan can be executed in a cost effective manner. The commenter noted that encryption has been the only presented solution provided by auditors and SDT guidance to protect both confidentiality and integrity for the data within this scope. The commenter noted that more resources and capital will be required for a 24-month implementation versus a phased-in implementation. The commenter further noted that a phased implementation provides the ability to not only ensure the most effective plan, but also provides the ability to plan more accurately within budget cycles. In addition, the commenter noted that if encryption fails, an entity would lose Real-time Assessment and Real-time monitoring and control data. The commenter expressed concern that a 24-month implementation timeline would impact reliability as there are many opportunities for encryption to fail that must be addressed. The commenter suggested that this has a direct correlation on cost when addressing those opportunities during this timeframe. Additionally, the commenter requested the SDT draft reference models of methods that do not require encryption as a method to protect communications between Control Centers.

CIP-012 is written in a non-prescriptive manner to allow entities to select the protection methods that most appropriately fit their organization. This allows for logical or physical protection as appropriate. Regarding guidance, the SDT encourages entities to draft and submit guidance on other implementation examples.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Proposed Revision to the Control Center Definition for the NERC Glossary of Terms

Project 2016-02 CIP MOD SDT

Current Control Center Definition

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, of: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for transmission Facilities at two or more locations, or 4) a Generator Operator for generation Facilities at two or more locations.

Proposed Revision to the Control Center Definition (Clean)

One or more facilities, including their associated data centers, that monitor and control the Bulk Electric System (BES) and also host operating personnel who:

1) perform the Real-time reliability-related tasks of a Reliability Coordinator; or
2) perform the Real-time reliability-related tasks of a Balancing Authority; or
3) perform the Real-time reliability-related tasks of a Transmission Operator for Transmission Facilities at two or more locations; or
4) can act independently as the Generator Operator to develop specific dispatch instructions for generation Facilities at two or more locations; or
5) can operate or direct the operation of a Transmission Owner's BES Transmission Facilities in Real-time.

Operating personnel do not include:

1) plant operators located at a generator plant site or personnel at a centrally located dispatch center who relay dispatch instructions without making any modifications; or
2) Transmission Owner or Transmission Operator field switching personnel.

Proposed Revision to the Control Center Definition (Redlined)

One or more facilities, including their associated data centers, ~~hosting operating personnel~~ that monitor and control the Bulk Electric System (BES) and also host operating personnel who:~~in real-time to~~

1) perform the Real-time reliability tasks~~,~~ of ~~including their associated data centers, of: 1)~~ a Reliability Coordinator; or~~,~~
2) perform the Real-time reliability tasks of a Balancing Authority; ~~-~~or~~,~~
3) perform the Real-time reliability tasks of a Transmission Operator for T~~t~~ransmission Facilities at two or more locations; or~~,~~

4) can act independently as ~~a~~the Generator Operator to develop specific dispatch instructions for generation Facilities at two or more locations; or~~,~~.

5) can operate or direct the operation of a Transmission Owner's BES Transmission Facilities in Real-time.

Operating personnel do not include:

1) plant operators located at a generator plant site or personnel at a centrally located dispatch center who relay dispatch instructions without making any modifications; or ~~and;~~

2) Transmission Owner or Transmission Operator field switching personnel.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Control Center Definition

Effective Date

Where approval by an applicable governmental authority is required, the NERC Glossary term "Control Center" shall become effective the first day of the first calendar quarter that is three (3) calendar months after the effective date of the applicable governmental authority's order approving the term, or as otherwise provided for by the applicable governmental authority.

Where approval by an applicable governmental authority is not required, the NERC Glossary term "Control Center" shall become effective on the first day of the first calendar quarter that is three (3) calendar months after the date the term is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Retirement Date

The existing NERC Glossary term "Control Center" shall be retired immediately prior to the effective date of the proposed NERC Glossary term "Control Center" in the particular jurisdiction in which the term is becoming effective.

Unofficial Comment Form

Project 2016-02 Modifications to CIP Standards
Glossary of Terms Used in NERC Reliability Standards – Control Center

Do not use this form for submitting comments. Use the Standards Balloting and Commenting System (SBS) to submit comments on **Project 2016-02 Modifications to NERC Glossary of Terms Used in Reliability Standards – Control Center.** Comments must be submitted by **8 p.m. Eastern, Monday, April 30, 2018.**

Additional information is available on the project page. If you have questions, contact Jordan Mallory at (404) 446-2589 or Mat Bunch at (404) 446-9785.

Background Information

On January 21, 2016, the Federal Energy Regulatory Commission (FERC) issued Order No. 822, which approved revisions to the cybersecurity Critical Infrastructure Protection (CIP) standards and directed NERC to develop certain modifications to requirements in the CIP standards. Specifically, FERC directed NERC to "develop modifications to the CIP Reliability Standards to require responsible entities to implement controls to protect, at a minimum, communication links and sensitive bulk electric system data communicated between bulk electric system Control Centers in a manner that is appropriately tailored to address the risks posed to the bulk electric system by the assets being protected (i.e., high, medium, or low impact)."

The Project 2016-02 Standard Drafting Team (SDT) developed proposed Reliability Standard CIP-012-1 to require Responsible Entities to implement controls to protect sensitive Bulk Electric System (BES) data or communications links between BES Control Centers and made the standard applicable to all impact levels due to the sensitivity of the data being communicated. As the FERC directive addressed the protection of data communicated between Control Centers, the SDT evaluated the current Control Center definition and identified the following opportunities for clarification:

- The term, "operating personnel" is not a NERC Glossary defined term and may be misinterpreted;
- The phrase, "two or more locations" may be overbroad;
- The phrase, "monitor and control" may be misinterpreted;
- The SDT members considered both the NERC Glossary defined term "Real-time" and undefined term "real-time."

To address the issues identified above, the SDT developed proposed modifications to the Control Center definition to make specific inclusions and exclusions. This model was based on the approach of the BES definition which also has specific inclusions and exclusions.

Current Control Center Definition:
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, of: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for transmission Facilities at two or more locations, or 4) a Generator Operator for generation Facilities at two or more locations.

Proposed Revised Control Center Definition:
One or more facilities, including their associated data centers, that monitor and control the Bulk Electric System (BES) and also host operating personnel who:

1) perform the Real-time reliability-related tasks of a Reliability Coordinator; or
2) perform the Real-time reliability-related tasks of a Balancing Authority; or
3) perform the Real-time reliability-related tasks of a Transmission Operator for Transmission Facilities at two or more locations; or
4) can act independently as the Generator Operator to develop specific dispatch instructions for generation Facilities at two or more locations; or
5) can operate or direct the operation of a Transmission Owner's BES Transmission Facilities in Real-time.

Operating personnel do not include:

1) plant operators located at a generator plant site or personnel at a centrally located dispatch center who relay dispatch instructions without making any modifications; or
2) Transmission Owner or Transmission Operator field switching personnel.

Proposed Revised Redline Control Center Definition:
One or more facilities, including their associated data centers, ~~hosting operating personnel~~ that monitor and control the Bulk Electric System (BES) and also host operating personnel who:~~in real-time to~~

1) perform the Real-time reliability tasks of~~,~~ ~~including their associated data centers, of: 1)~~ a Reliability Coordinator~~,~~' or
2) ~~2)~~ perform the Real-time reliability tasks of a Balancing Authority;~~,~~ or
3) ~~3)~~ perform the Real-time reliability tasks of a Transmission Operator for T~~t~~ransmission Facilities at two or more locations;~~,~~ or
4) ~~4)~~ can act independently as the~~a~~ Generator Operator to develop specific dispatch instructions for generation Facilities at two or more locations; or~~.~~
5) can operate or direct the operation of a Transmission Owner's BES Transmission Facilities in Real-time.

Operating personnel do not include:

1) plant operators located at a generator plant site or personnel at a centrally located dispatch center who relay dispatch instructions without making any modifications; or
2) Transmission Owner or Transmission Operator field switching personnel.

Questions

1. Control Center definition: Do you agree with the proposed revisions to the definition of Control Center? If not, please provide rationale or propose an alternative definition.

   ☐ Yes
   ☐ No

   Comments:

2. Control Center definition: Do the proposed revisions to the Control Center definition change the scope or intent of any current or pending Reliability Standard(s) using the defined term (examples include Reliability Standards: COM-001-3; TOP-001-4; and IRO-002-5)? If yes, provide details of the affected Reliability Standard(s), requirements, and any anticipated impact.

   ☐ Yes
   ☐ No

   Comments:

3. Control Center definition: The SDT contends that there will be no change in BES Cyber System categorization by clarifying the definition of Control Center. This assertion is based on SDT review of the CIP-002-5.1a criteria and its understanding of BES Cyber System categorization through experience implementing CIP-002-5.1a. Do you agree with this assertion? If not, please provide rationale and practical examples of where a change in categorization will occur as a result of this modification.

   ☐ Yes
   ☐ No

   Comments:

4. Control Center definition: Is there a scenario where a Control Center hosts both the inclusion personnel and the exclusion personnel? If yes, please provide them here.

   ☐ Yes
   ☐ No

   Comments:

5. Implementation Plan: The new Control Center definition will become effective on the first day of the first calendar quarter that is three (3) calendar months after the effective date of the applicable governmental authority's order approving the term, or as otherwise provided for by the applicable governmental authority. Do you agree that three calendar months is enough time to update documentation? If you do not agree, please provide the amount of time needed and types of actions that will need to be completed during this time.

   ☐ Yes
   ☐ No

   Comments:

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Reminder

Project 2016-02 Modifications to CIP Standards

Initial and Additional Ballots and Non-binding Polls Open through April 30, 2018

Now Available

Initial ballots for the **Control Center Definition** and its **Implementation Plan**, additional ballots for **CIP-002-6** and **CIP-012-1** and the associated non-binding polls of the associated Violation Risk Factors and Violation Severity Levels are open through **8 p.m. Eastern, Monday, April 30, 2018.**

The standard drafting team's considerations of the responses received from the last comment period for **CIP-002-6** and **CIP-012-1** are reflected in these drafts of the standards.

Balloting

Members of the ballot pools associated with this project can log in and submit their votes by accessing the Standards Balloting and Commenting System (SBS) here. If you experience any difficulties navigating the SBS, contact Wendy Muller.

- *If you are having difficulty accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out, contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern).*
- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*
- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Note: If a member cast a vote in the previous ballot, that vote will not carry over to the additional ballot. It is the responsibility of the registered voter in the ballot pool to cast a vote again in the additional ballot. To ensure a quorum is reached, if you do not want to vote affirmative or negative, cast an abstention.

Next Steps

The ballot results will be announced and posted on the project page. The drafting team will review all responses received during the comment period and determine the next steps of the project.

For information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact Mat Bunch at (404) 446-9785 or Jordan Mallory at (404) 446-2589.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2016-02 Modifications to CIP Standards

Formal Comment Periods Open through April 30, 2018
Ballot Pools Forming through April 16, 2018

Now Available

Three formal comment periods are open through **8 p.m. Eastern, Monday, April 30, 2018** for:

1. **CIP-002-6 – Cyber Security - BES Cyber System Categorization**
2. **CIP-012-1 – Cyber Security - Communications between Control Centers**
3. **Project 2016-02 Modifications to NERC Glossary of Terms Used in Reliability Standards – Control Center**

Commenting

Use the Standards Balloting and Commenting System (SBS) to submit comments. If you experience difficulties navigating the SBS, contact Wendy Muller. Unofficial Word versions of the comment forms are posted on the project page.

Ballot Pools

Ballot pools are being formed through **8 p.m. Eastern, Monday, April 16, 2018** for the **Control Center Definition** and its **Implementation Plan**. Registered Ballot Body members can join the ballot pools here.

- *If you are having difficulty accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out, contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern).*
- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*
- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Next Steps

The initial ballots for the **Control Center Definition** and its **Implementation Plan** will be conducted **April 20-30, 2018**. Additional ballots for **CIP-002-6** and **CIP-012-1** and the associated non-binding polls of the associated Violation Risk Factors and Violation Severity Levels will be conducted **April 20-30, 2018.**

For information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact Mat Bunch at (404) 446-9785 or Jordan Mallory at (404) 446-2589.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/132)
Ballot Name: 2016-02 Modifications to CIP Standards Control Center Definiton IN 1 DEF
Voting Start Date: 4/20/2018 12:01:00 AM
Voting End Date: 4/30/2018 8:00:00 PM
Ballot Type: DEF
Ballot Activity: IN
Ballot Series: 1
Total # Votes: 244
Total Ballot Pool: 300
Quorum: 81.33
Weighted Segment Value: 46.71

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	75	1	36	0.643	20	0.357	0	7	12
Segment: 2	5	0.4	4	0.4	0	0	0	1	0
Segment: 3	70	1	27	0.54	23	0.46	0	5	15
Segment: 4	22	1	6	0.316	13	0.684	0	0	3
Segment: 5	71	1	25	0.481	27	0.519	1	3	15

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 6	49	1	15	0.417	21	0.583	0	2	11
Segment: 7	0	0	0	0	0	0	0	0	0
Segment: 8	1	0.1	0	0	1	0.1	0	0	0
Segment: 9	1	0.1	0	0	1	0.1	0	0	0
Segment: 10	6	0.6	1	0.1	5	0.5	0	0	0
Totals:	300	6.2	114	2.896	111	3.304	1	18	56

BALLOT POOL MEMBERS

Show All entries

Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Allete - Minnesota Power, Inc.	Jamie Monette		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Ameren - Ameren Services	Eric Scott		Negative	Comments Submitted
1	American Transmission Company, LLC	Douglas Johnson		Negative	Comments Submitted
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Joe Tarantino	Affirmative	N/A
1	Basin Electric Power Cooperative	David Rudolph		None	N/A
1	BC Hydro and Power Authority	Patricia Robertson		Affirmative	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Negative	Comments Submitted
1	Bonneville Power Administration	Kammy Rogers-Holliday		Negative	Comments Submitted
1	Cedar Falls Utilities	Adam Peterson		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Hudson Gas & Electric Corp.	Frank Pace		Negative	Third-Party Comments
1	City Utilities of Springfield, Missouri	Michael Buyce		Affirmative	N/A
1	CMS Energy - Consumers Energy Company	James Anderson		Negative	Comments Submitted
1	Colorado Springs Utilities	Devin Elverdi		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Comments Submitted
1	CPS Energy	Gladys DeLaO		None	N/A
1	Duke Energy	Laura Lee		Negative	Comments Submitted
1	East Kentucky Power Cooperative	Amber Skillern		Affirmative	N/A
1	Edison International - Southern California Edison Company	Steven Mavis		Negative	Comments Submitted
1	Entergy - Entergy Services, Inc.	Oliver Burke		Negative	Comments Submitted
1	Eversource Energy	Quintin Lee		Affirmative	N/A
1	Exelon	Chris Scanlon		Negative	Comments Submitted
1	FirstEnergy - FirstEnergy Corporation	Karen Yoder		Affirmative	N/A
1	Gainesville Regional Utilities	David Owens	Brandon McCormick	Negative	Comments Submitted
1	Great Plains Energy - Kansas City Power and Light Co.	James McBee	Douglas Webb	Affirmative	N/A
1	Great River Energy	Gordon Pietsch		None	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Affirmative	N/A
1	IDACORP - Idaho Power Company	Laura Nelson		None	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Stephanie Burns	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	JEA	Ted Hobson	Joe McClung	Affirmative	N/A
1	KAMO Electric Cooperative	Walter Kenyon		None	N/A
1	Lakeland Electric	Larry Watt		Negative	Comments Submitted
1	Long Island Power Authority	Robert Ganley		None	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		Affirmative	N/A
1	Lower Colorado River Authority	Michael Shaw		Abstain	N/A
1	Manitoba Hydro	Mike Smith		Affirmative	N/A
1	MEAG Power	David Weekley	Scott Miller	Abstain	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard		None	N/A
1	Muscatine Power and Water	Andy Kurriger		Affirmative	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Affirmative	N/A
1	Network and Security Technologies	Nicholas Lauriat		Affirmative	N/A
1	New York Power Authority	Salvatore Spagnolo		Negative	Third-Party Comments
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Affirmative	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Oncor Electric Delivery	Lee Maurer	Tho Tran	Affirmative	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		Negative	Third-Party Comments
1	PNM Resources - Public Service Company of New Mexico	Laurie Williams		Negative	Comments Submitted
1	Portland General Electric Co.	Nathaniel Clague		Abstain	N/A
1	PPL Electric Utilities Corporation	Brenda Truhe		Affirmative	N/A
1	PSEG - Public Service Electric and Gas Co.	Joseph Smith		Affirmative	N/A
1	Public Utility District No. 1 of Pend Oreille County	Kevin Conway		None	N/A
1	Public Utility District No. 1 of Snohomish County	Long Duong		Affirmative	N/A
1	Sacramento Municipal Utility District	Arthur Starkovich	Joe Tarantino	Affirmative	N/A
1	Salt River Project	Steven Cobb		None	N/A
1	Santee Cooper	Chris Wagner		None	N/A
1	SCANA - South Carolina Electric and Gas Co.	Tom Hanzlik		None	N/A
1	Seattle City Light	Pawel Krupa		Negative	Comments Submitted
1	Seminole Electric Cooperative, Inc.	Mark Churilla		Abstain	N/A
1	Sho-Me Power Electric Cooperative	Peter Dawson		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Katherine Prewitt		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Southern Indiana Gas and Electric Co.	Steve Rawlinson		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Abstain	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell		Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	Howell Scott		Affirmative	N/A
1	Tri-State G and T Association, Inc.	Tracy Sliman		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Westar Energy	Kevin Giles		Affirmative	N/A
1	Western Area Power Administration	sean erickson		Negative	Comments Submitted
1	Wind Energy Transmission Texas, LLC	Julius Horvath		None	N/A
1	Xcel Energy, Inc.	Dean Schiro		Affirmative	N/A
2	Electric Reliability Council of Texas, Inc.	Brandon Gleason		Affirmative	N/A
2	Independent Electricity System Operator	Leonard Kula		Affirmative	N/A
2	Midcontinent ISO, Inc.	Ellen Oswald		Affirmative	N/A
2	New York Independent System Operator	Gregory Campoli		Abstain	N/A
2	PJM Interconnection, L.L.C.	Mark Holman		Affirmative	N/A
3	Ameren - Ameren Services	David Jendras		Negative	Comments Submitted
3	APS - Arizona Public Service Co.	Vivian Vo		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Arkansas Electric Cooperative Corporation	Philip Huff		Negative	Third-Party Comments
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	W. Dwayne Preston		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney	Brad Calbick	None	N/A
3	Basin Electric Power Cooperative	Jeremy Voll		Negative	Third-Party Comments
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Annette Johnston	Darnez Gresham	Negative	Comments Submitted
3	Black Hills Corporation	Eric Egge		Affirmative	N/A
3	Bonneville Power Administration	Rebecca Berdahl		Negative	Comments Submitted
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City of Farmington	Linda Jacobson-Quinn		Affirmative	N/A
3	City of Independence, Power and Light Department	Mike Lotz		None	N/A
3	City of Vero Beach	Ginny Beigel	Brandon McCormick	Negative	Comments Submitted
3	City Utilities of Springfield, Missouri	Scott Williams		Affirmative	N/A
3	Cleco Corporation	Michelle Corley	Louis Guidry	None	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Colorado Springs Utilities	Hillary Dobson		Affirmative	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Comments Submitted
3	CPS Energy	James Grimshaw		None	N/A
3	DTE Energy - Detroit Edison Company	Karie Barczak		None	N/A
3	Duke Energy	Lee Schuster		Affirmative	N/A
3	East Kentucky Power Cooperative	Patrick Woods		Affirmative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Eversource Energy	Mark Kenny		Affirmative	N/A
3	Exelon	John Bee		Negative	Comments Submitted
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		None	N/A
3	Florida Municipal Power Agency	Joe McKinney	Brandon McCormick	Negative	Comments Submitted
3	Georgia System Operations Corporation	Scott McGough		Negative	Third-Party Comments
3	Great Plains Energy - Kansas City Power and Light Co.	John Carlson	Douglas Webb	Affirmative	N/A
3	Great River Energy	Brian Glover		Negative	Third-Party Comments
3	KAMO Electric Cooperative	Ted Hilmes		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Lincoln Electric System	Jason Fortik		Negative	Third-Party Comments
3	Los Angeles Department of Water and Power	Henry (Hank) Williams		None	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	Manitoba Hydro	Karim Abdel-Hadi		Affirmative	N/A
3	MEAG Power	Roger Brand	Scott Miller	Abstain	N/A
3	Muscatine Power and Water	Seth Shoemaker		Negative	Third-Party Comments
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Negative	Comments Submitted
3	New York Power Authority	David Rivera		Negative	Third-Party Comments
3	NiSource - Northern Indiana Public Service Co.	Aimee Harris		Affirmative	N/A
3	North Carolina Electric Membership Corporation	doug white	Scott Brame	Negative	Third-Party Comments
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Affirmative	N/A
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen		None	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	OTP - Otter Tail Power Company	Wendi Olson		Negative	Third-Party Comments
3	Owensboro Municipal Utilities	Thomas Lyons		None	N/A
3	Platte River Power Authority	Jeff Landis		Abstain	N/A
3	PNM Resources - Public Service Company of New Mexico	Lynn Goldstein		Negative	Comments Submitted
3	Portland General Electric Co.	Angela Gaines		Abstain	N/A
3	PPL - Louisville Gas and Electric Co.	Charles Freibert		Affirmative	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Abstain	N/A
3	Public Utility District No. 1 of Pend Oreille County	Amber Orr		None	N/A
3	Rutherford EMC	Tom Haire		None	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Joe Tarantino	Affirmative	N/A
3	Salt River Project	Robert Kondziolka		Negative	Third-Party Comments
3	Santee Cooper	James Poston		None	N/A
3	SCANA - South Carolina Electric and Gas Co.	Scott Parker		None	N/A
3	Seminole Electric Cooperative, Inc.	James Frauen		Abstain	N/A
3	Sho-Me Power Electric Cooperative	Jeff Neas		Affirmative	N/A
3	Snohomish County PUD No. 1	Mark Oens		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Southern Company - Alabama Power Company	Joel Dembowski		Negative	Comments Submitted
3	Southern Indiana Gas and Electric Co.	Fred Frederick		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson		Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		None	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Comments Submitted
3	Westar Energy	Bo Jones		Affirmative	N/A
3	Xcel Energy, Inc.	Michael Ibold		Affirmative	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		None	N/A
4	American Public Power Association	Jack Cashin		Negative	Comments Submitted
4	Arkansas Electric Cooperative Corporation	Alice Wright		Negative	Third-Party Comments
4	Austin Energy	Esther Weekes		Affirmative	N/A
4	City of Poplar Bluff	Neal Williams		None	N/A
4	City Utilities of Springfield, Missouri	John Allen		Affirmative	N/A
4	CMS Energy - Consumers Energy Company	Theresa Martinez		Negative	Third-Party Comments
4	FirstEnergy - FirstEnergy Corporation	Aubrey Short		Affirmative	N/A
4	Florida Municipal Power Agency	Carol Chinn	Brandon McCormick	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Georgia System Operations Corporation	Guy Andrews		Negative	Third-Party Comments
4	Illinois Municipal Electric Agency	Mary Ann Todd		None	N/A
4	Indiana Municipal Power Agency	Jack Alvey	Scott Berry	Negative	Third-Party Comments
4	LaGen	Richard Comeaux		Negative	Third-Party Comments
4	MGE Energy - Madison Gas and Electric Co.	Joseph DePoorter		Negative	Third-Party Comments
4	National Rural Electric Cooperative Association	Barry Lawson		Negative	Comments Submitted
4	North Carolina Electric Membership Corporation	John Lemire	Scott Brame	Negative	Third-Party Comments
4	Public Utility District No. 1 of Snohomish County	John Martinsen		Affirmative	N/A
4	Sacramento Municipal Utility District	Beth Tincher	Joe Tarantino	Affirmative	N/A
4	Seattle City Light	Hao Li		Negative	Comments Submitted
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho		Affirmative	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Negative	Comments Submitted
4	WEC Energy Group, Inc.	Anthony Jankowski		Negative	Comments Submitted
5	Acciona Energy North America	George Brown		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	AEP	Thomas Foltz		Affirmative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Negative	Comments Submitted
5	APS - Arizona Public Service Co.	Kelsi Rigby		Affirmative	N/A
5	Arkansas Electric Cooperative Corporation	Moses Harris		Negative	Third-Party Comments
5	Associated Electric Cooperative, Inc.	Brad Haralson		None	N/A
5	Austin Energy	Shirley Mathew		None	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	Basin Electric Power Cooperative	Mike Kraft		Negative	Third-Party Comments
5	BC Hydro and Power Authority	Helen Hamilton Harding		None	N/A
5	Berkshire Hathaway - NV Energy	Kevin Salsbury		Negative	Comments Submitted
5	Black Hills Corporation	George Tatar		Affirmative	N/A
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		Negative	Third-Party Comments
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	Brazos Electric Power Cooperative, Inc.	Shari Heino		Negative	Third-Party Comments
5	California Department of Water Resources	ASM Mostafa		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Negative	Third-Party Comments
5	City Water, Light and Power of Springfield, IL	Steve Rose		Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Negative	Comments Submitted
5	Colorado Springs Utilities	Jeff Icke		Affirmative	N/A
5	Dairyland Power Cooperative	Tommy Drea		None	N/A
5	Dominion - Dominion Resources, Inc.	Lou Oberski		Negative	Comments Submitted
5	DTE Energy - Detroit Edison Company	Jeffrey DePriest		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Negative	Comments Submitted
5	East Kentucky Power Cooperative	Steve Ricker		Affirmative	N/A
5	Entergy	Jamie Prater		Negative	Comments Submitted
5	Exelon	Ruth Miller		Negative	Comments Submitted
5	FirstEnergy - FirstEnergy Solutions	Robert Loy		Affirmative	N/A
5	Florida Municipal Power Agency	Chris Gowder	Brandon McCormick	Negative	Comments Submitted
5	Great Plains Energy - Kansas City Power and Light Co.	Harold Wyble	Douglas Webb	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Great River Energy	Preston Walsh		Negative	Third-Party Comments
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	JEA	John Babik		None	N/A
5	Kissimmee Utility Authority	Mike Blough	Brandon McCormick	Negative	Comments Submitted
5	Lakeland Electric	Jim Howard		None	N/A
5	Lincoln Electric System	Kayleigh Wilkerson		Negative	Third-Party Comments
5	Manitoba Hydro	Yuguang Xiao		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	David Gordon		Negative	Third-Party Comments
5	MEAG Power	Steven Grego	Scott Miller	Abstain	N/A
5	Muscatine Power and Water	Neal Nelson		Affirmative	N/A
5	NaturEner USA, LLC	Eric Smith		None	N/A
5	NB Power Corporation	Laura McLeod		Affirmative	N/A
5	Nebraska Public Power District	Don Schmit		Negative	Third-Party Comments
5	New York Power Authority	Erick Barrios		Negative	Third-Party Comments
5	NiSource - Northern Indiana Public Service Co.	Dmitriy Bazylyuk		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	North Carolina Electric Membership Corporation	Robert Beadle	Scott Brame	Negative	Third-Party Comments
5	OGE Energy - Oklahoma Gas and Electric Co.	John Rhea		Negative	Comments Submitted
5	Omaha Public Power District	Mahmood Safi		Negative	Third-Party Comments
5	Orlando Utilities Commission	Richard Kinas		None	N/A
5	OTP - Otter Tail Power Company	Cathy Fogale		Negative	Third-Party Comments
5	Platte River Power Authority	Tyson Archie		Affirmative	N/A
5	Portland General Electric Co.	Ryan Olson		Abstain	N/A
5	PPL - Louisville Gas and Electric Co.	JULIE HOSTRANDER		Affirmative	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Affirmative	N/A
5	Public Utility District No. 1 of Chelan County	Haley Sousa		Abstain	N/A
5	Public Utility District No. 1 of Pend Oreille County	Mark Cleveland		None	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Sacramento Municipal Utility District	Susan Oto	Joe Tarantino	Affirmative	N/A
5	Salt River Project	Kevin Nielsen		Negative	Third-Party Comments
5	Santee Cooper	Tommy Curtis		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	SCANA - South Carolina Electric and Gas Co.	Alyssa Hubbard		None	N/A
5	Silicon Valley Power - City of Santa Clara	Sandra Pacheco		None	N/A
5	Southern Company - Southern Company Generation	William D. Shultz		Negative	Comments Submitted
5	Southern Indiana Gas and Electric Co.	Mark McDonald		Affirmative	N/A
5	SunPower	Bradley Collard		None	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin		None	N/A
5	Tennessee Valley Authority	M Lee Thomas		Affirmative	N/A
5	Tri-State G and T Association, Inc.	Mark Stein		Negative	No Comment Submitted
5	U.S. Bureau of Reclamation	Wendy Center		Affirmative	N/A
5	WEC Energy Group, Inc.	Linda Horn		Negative	Comments Submitted
5	Xcel Energy, Inc.	Gerry Huitt		Affirmative	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Negative	Comments Submitted
6	APS - Arizona Public Service Co.	Jonathan Aragon		Affirmative	N/A
6	Arkansas Electric Cooperative Corporation	Bruce Walkup		Negative	Third-Party Comments
6	Associated Electric Cooperative, Inc.	Brian Ackermann		Affirmative	N/A
6	Basin Electric Power Cooperative	Paul Huettl		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Black Hills Corporation	Eric Scherr		None	N/A
6	Bonneville Power Administration	Andrew Meyers		Negative	Comments Submitted
6	Cleco Corporation	Robert Hirchak	Louis Guidry	None	N/A
6	Colorado Springs Utilities	Shannon Fair		Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Robert Winston		Negative	Comments Submitted
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
6	Duke Energy	Greg Cecil		Negative	Comments Submitted
6	Edison International - Southern California Edison Company	Kenya Streeter		Negative	Comments Submitted
6	Entergy	Julie Hall		Negative	Comments Submitted
6	Exelon	Becky Webb		Negative	Comments Submitted
6	FirstEnergy - FirstEnergy Solutions	Ann Ivanc		Affirmative	N/A
6	Florida Municipal Power Agency	Richard Montgomery	Brandon McCormick	Negative	Comments Submitted
6	Florida Municipal Power Pool	Tom Reedy	Brandon McCormick	Negative	Comments Submitted
6	Great Plains Energy - Kansas City Power and Light Co.	Jennifer Flandermeyer	Douglas Webb	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Great River Energy	Donna Stephenson	Michael Brytowski	Negative	Third-Party Comments
6	Los Angeles Department of Water and Power	Anton Vu		Affirmative	N/A
6	Manitoba Hydro	Blair Mukanik		None	N/A
6	Muscatine Power and Water	Ryan Streck	Amie Shuger McConnaha	Negative	Third-Party Comments
6	New York Power Authority	Shivaz Chopra	Shelly Dineen	Negative	Third-Party Comments
6	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joe O'Brien		Affirmative	N/A
6	Northern California Power Agency	Dennis Sismaet		Negative	Comments Submitted
6	NRG - NRG Energy, Inc.	Martin Sidor		None	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay		Negative	Third-Party Comments
6	Portland General Electric Co.	Daniel Mason		None	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
6	PSEG - PSEG Energy Resources and Trade LLC	Karla Barton		None	N/A
6	Public Utility District No. 1 of Chelan County	Davis Jelusich		Abstain	N/A
6	Public Utility District No. 1 of Pend Oreille County	Kimberly Gentle		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Public Utility District No. 2 of Grant County, Washington	LeRoy Patterson		None	N/A
6	Sacramento Municipal Utility District	Jamie Cutlip	Joe Tarantino	Affirmative	N/A
6	Salt River Project	Bobby Olsen		Negative	Third-Party Comments
6	Santee Cooper	Michael Brown		None	N/A
6	SCANA - South Carolina Electric and Gas Co.	John Folsom		None	N/A
6	Seattle City Light	Charles Freeman		None	N/A
6	Seminole Electric Cooperative, Inc.	Trudy Novak		Abstain	N/A
6	Snohomish County PUD No. 1	Franklin Lu		Affirmative	N/A
6	Southern Company - Southern Company Generation and Energy Marketing	Jennifer Sykes		Negative	Comments Submitted
6	Tacoma Public Utilities (Tacoma, WA)	Rick Applegate		Affirmative	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Affirmative	N/A
6	WEC Energy Group, Inc.	David Hathaway		Negative	Comments Submitted
6	Westar Energy	Megan Wagner		Affirmative	N/A
6	Western Area Power Administration	Charles Faust		Negative	Comments Submitted
6	Xcel Energy, Inc.	Carrie Dixon		Affirmative	N/A
8	David Kiguel	David Kiguel		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson		Negative	Third-Party Comments
10	Midwest Reliability Organization	Russel Mountjoy		Negative	Comments Submitted
10	New York State Reliability Council	ALAN ADAMSON		Negative	Comments Submitted
10	Northeast Power Coordinating Council	Guy V. Zito		Negative	Comments Submitted
10	ReliabilityFirst	Anthony Jablonski		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Negative	Comments Submitted
10	Western Electricity Coordinating Council	Steven Rueckert		Negative	Comments Submitted

Previous 1 Next

Showing 1 to 300 of 300 entries

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/132)
Ballot Name: 2016-02 Modifications to CIP Standards Control Center Definiton Implementation Plan IN 1 OT
Voting Start Date: 4/20/2018 12:01:00 AM
Voting End Date: 4/30/2018 8:00:00 PM
Ballot Type: OT
Ballot Activity: IN
Ballot Series: 1
Total # Votes: 243
Total Ballot Pool: 298
Quorum: 81.54
Weighted Segment Value: 37.98

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	74	1	29	0.527	26	0.473	0	7	12
Segment: 2	5	0.4	1	0.1	3	0.3	0	1	0
Segment: 3	70	1	19	0.38	31	0.62	0	5	15
Segment: 4	22	1	5	0.294	12	0.706	0	1	4
Segment: 5	70	1	23	0.434	30	0.566	0	3	14
Segment: 6	49	1	15	0.405	22	0.595	0	2	10
Segment: 7	0	0	0	0	0	0	0	0	0
Segment: 8	1	0.1	0	0	1	0.1	0	0	0
Segment: 9	1	0.1	0	0	1	0.1	0	0	0
Segment: 10	6	0.3	1	0.1	2	0.2	0	3	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Totals:	298	5.9	93	2.241	128	3.659	0	22	55

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Allete - Minnesota Power, Inc.	Jamie Monette		Abstain	N/A
1	Ameren - Ameren Services	Eric Scott		Negative	Comments Submitted
1	American Transmission Company, LLC	Douglas Johnson		Negative	Comments Submitted
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Joe Tarantino	Affirmative	N/A
1	Basin Electric Power Cooperative	David Rudolph		None	N/A
1	BC Hydro and Power Authority	Patricia Robertson		Affirmative	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Negative	Comments Submitted
1	Bonneville Power Administration	Kammy Rogers-Holliday		Affirmative	N/A
1	Cedar Falls Utilities	Adam Peterson		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Negative	Third-Party Comments
1	Central Hudson Gas & Electric Corp.	Frank Pace		Negative	Third-Party Comments
1	City Utilities of Springfield, Missouri	Michael Buyce		Negative	Third-Party Comments
1	CMS Energy - Consumers Energy Company	James Anderson		Negative	Comments Submitted
1	Colorado Springs Utilities	Devin Elverdi		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Comments Submitted
1	CPS Energy	Gladys DeLaO		None	N/A
1	Duke Energy	Laura Lee		Negative	Comments Submitted
1	East Kentucky Power Cooperative	Amber Skillern		Affirmative	N/A
1	Edison International - Southern California Edison Company	Steven Mavis		Negative	Comments Submitted
1	Entergy - Entergy Services, Inc.	Oliver Burke		Negative	Comments Submitted
1	Eversource Energy	Quintin Lee		Affirmative	N/A
1	Exelon	Chris Scanlon		Negative	Comments Submitted
1	FirstEnergy - FirstEnergy Corporation	Karen Yoder		Affirmative	N/A
1	Great Plains Energy - Kansas City Power and Light Co.	James McBee	Douglas Webb	Affirmative	N/A
1	Great River Energy	Gordon Pietsch		None	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Affirmative	N/A
1	IDACORP - Idaho Power Company	Laura Nelson		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	International Transmission Company Holdings Corporation	Michael Moltane	Stephanie Burns	Negative	Comments Submitted
1	JEA	Ted Hobson	Joe McClung	Affirmative	N/A
1	KAMO Electric Cooperative	Walter Kenyon		None	N/A
1	Lakeland Electric	Larry Watt		Negative	Comments Submitted
1	Long Island Power Authority	Robert Ganley		None	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		Affirmative	N/A
1	Lower Colorado River Authority	Michael Shaw		Abstain	N/A
1	Manitoba Hydro	Mike Smith		Affirmative	N/A
1	MEAG Power	David Weekley	Scott Miller	Abstain	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard		None	N/A
1	Muscatine Power and Water	Andy Kurriger		Negative	Third-Party Comments
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Negative	Third-Party Comments
1	National Grid USA	Michael Jones		Affirmative	N/A
1	Network and Security Technologies	Nicholas Lauriat		Affirmative	N/A
1	New York Power Authority	Salvatore Spagnolo		Negative	Third-Party Comments
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Affirmative	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Negative	Comments Submitted
1	Oncor Electric Delivery	Lee Maurer	Tho Tran	Affirmative	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	PNM Resources - Public Service Company of New Mexico	Laurie Williams		Negative	Comments Submitted
1	Portland General Electric Co.	Nathaniel Clague		Abstain	N/A
1	PPL Electric Utilities Corporation	Brenda Truhe		Affirmative	N/A
1	PSEG - Public Service Electric and Gas Co.	Joseph Smith		Affirmative	N/A
1	Public Utility District No. 1 of Pend Oreille County	Kevin Conway		None	N/A
1	Public Utility District No. 1 of Snohomish County	Long Duong		Affirmative	N/A
1	Sacramento Municipal Utility District	Arthur Starkovich	Joe Tarantino	Affirmative	N/A
1	Salt River Project	Steven Cobb		None	N/A
1	Santee Cooper	Chris Wagner		None	N/A
1	SCANA - South Carolina Electric and Gas Co.	Tom Hanzlik		None	N/A
1	Seattle City Light	Pawel Krupa		Negative	Comments Submitted
1	Seminole Electric Cooperative, Inc.	Mark Churilla		Abstain	N/A
1	Sho-Me Power Electric Cooperative	Peter Dawson		Negative	Third-Party Comments
1	Southern Company - Southern Company Services, Inc.	Katherine Prewitt		Negative	Comments Submitted
1	Southern Indiana Gas and Electric Co.	Steve Rawlinson		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Abstain	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell		Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Tennessee Valley Authority	Howell Scott		Affirmative	N/A
1	Tri-State G and T Association, Inc.	Tracy Sliman		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Negative	Comments Submitted
1	Westar Energy	Kevin Giles		Affirmative	N/A
1	Western Area Power Administration	sean erickson		Negative	Comments Submitted
1	Wind Energy Transmission Texas, LLC	Julius Horvath		None	N/A
1	Xcel Energy, Inc.	Dean Schiro		Affirmative	N/A
2	Electric Reliability Council of Texas, Inc.	Brandon Gleason		Negative	Comments Submitted
2	Independent Electricity System Operator	Leonard Kula		Negative	Comments Submitted
2	Midcontinent ISO, Inc.	Ellen Oswald		Negative	Comments Submitted
2	New York Independent System Operator	Gregory Campoli		Abstain	N/A
2	PJM Interconnection, L.L.C.	Mark Holman		Affirmative	N/A
3	Ameren - Ameren Services	David Jendras		Negative	Comments Submitted
3	APS - Arizona Public Service Co.	Vivian Vo		Affirmative	N/A
3	Arkansas Electric Cooperative Corporation	Philip Huff		Negative	Third-Party Comments
3	Associated Electric Cooperative, Inc.	Todd Bennett		Negative	Comments Submitted
3	Austin Energy	W. Dwayne Preston		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney	Brad Calbick	None	N/A
3	Basin Electric Power Cooperative	Jeremy Voll		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Annette Johnston	Darnez Gresham	Negative	Comments Submitted
3	Black Hills Corporation	Eric Egge		Affirmative	N/A
3	Bonneville Power Administration	Rebecca Berdahl		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Negative	Third-Party Comments
3	City of Farmington	Linda Jacobson-Quinn		Affirmative	N/A
3	City of Independence, Power and Light Department	Mike Lotz		None	N/A
3	City of Vero Beach	Ginny Beigel	Brandon McCormick	Negative	Comments Submitted
3	City Utilities of Springfield, Missouri	Scott Williams		Negative	Third-Party Comments
3	Cleco Corporation	Michelle Corley	Louis Guidry	None	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Negative	Comments Submitted
3	Colorado Springs Utilities	Hillary Dobson		Affirmative	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Comments Submitted
3	CPS Energy	James Grimshaw		None	N/A
3	DTE Energy - Detroit Edison Company	Karie Barczak		None	N/A
3	Duke Energy	Lee Schuster		Negative	Comments Submitted
3	East Kentucky Power Cooperative	Patrick Woods		Affirmative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Eversource Energy	Mark Kenny		Affirmative	N/A
3	Exelon	John Bee		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		None	N/A
3	Florida Municipal Power Agency	Joe McKinney	Brandon McCormick	Negative	Comments Submitted
3	Georgia System Operations Corporation	Scott McGough		Negative	Third-Party Comments
3	Great Plains Energy - Kansas City Power and Light Co.	John Carlson	Douglas Webb	Affirmative	N/A
3	Great River Energy	Brian Glover		Negative	Third-Party Comments
3	KAMO Electric Cooperative	Ted Hilmes		None	N/A
3	Lincoln Electric System	Jason Fortik		Negative	Third-Party Comments
3	Los Angeles Department of Water and Power	Henry (Hank) Williams		None	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Negative	Third-Party Comments
3	Manitoba Hydro	Karim Abdel-Hadi		Affirmative	N/A
3	MEAG Power	Roger Brand	Scott Miller	Abstain	N/A
3	Muscatine Power and Water	Seth Shoemaker		Negative	Third-Party Comments
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Negative	Comments Submitted
3	New York Power Authority	David Rivera		Negative	Third-Party Comments
3	NiSource - Northern Indiana Public Service Co.	Aimee Harris		Negative	Comments Submitted
3	North Carolina Electric Membership Corporation	doug white	Scott Brame	Negative	Third-Party Comments
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	NW Electric Power Cooperative, Inc.	John Stickley		Negative	Third-Party Comments
3	Ocala Utility Services	Neville Bowen		None	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Negative	Third-Party Comments
3	OTP - Otter Tail Power Company	Wendi Olson		Negative	Third-Party Comments
3	Owensboro Municipal Utilities	Thomas Lyons		None	N/A
3	Platte River Power Authority	Jeff Landis		Abstain	N/A
3	PNM Resources - Public Service Company of New Mexico	Lynn Goldstein		Negative	Comments Submitted
3	Portland General Electric Co.	Angela Gaines		Abstain	N/A
3	PPL - Louisville Gas and Electric Co.	Charles Freibert		Affirmative	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Abstain	N/A
3	Public Utility District No. 1 of Pend Oreille County	Amber Orr		None	N/A
3	Rutherford EMC	Tom Haire		None	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Joe Tarantino	Affirmative	N/A
3	Salt River Project	Robert Kondziolka		Negative	Third-Party Comments
3	Santee Cooper	James Poston		None	N/A
3	SCANA - South Carolina Electric and Gas Co.	Scott Parker		None	N/A
3	Seminole Electric Cooperative, Inc.	James Frauen		Abstain	N/A
3	Sho-Me Power Electric Cooperative	Jeff Neas		Negative	Third-Party Comments
3	Snohomish County PUD No. 1	Mark Oens		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Southern Company - Alabama Power Company	Joel Dembowski		Negative	Comments Submitted
3	Southern Indiana Gas and Electric Co.	Fred Frederick		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson		Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		None	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Comments Submitted
3	Westar Energy	Bo Jones		Affirmative	N/A
3	Xcel Energy, Inc.	Michael Ibold		Affirmative	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		None	N/A
4	American Public Power Association	Jack Cashin		None	N/A
4	Arkansas Electric Cooperative Corporation	Alice Wright		Negative	Third-Party Comments
4	Austin Energy	Esther Weekes		Affirmative	N/A
4	City of Poplar Bluff	Neal Williams		None	N/A
4	City Utilities of Springfield, Missouri	John Allen		Negative	Third-Party Comments
4	CMS Energy - Consumers Energy Company	Theresa Martinez		Negative	Third-Party Comments
4	FirstEnergy - FirstEnergy Corporation	Aubrey Short		Affirmative	N/A
4	Florida Municipal Power Agency	Carol Chinn	Brandon McCormick	Negative	Comments Submitted
4	Georgia System Operations Corporation	Guy Andrews		Negative	Third-Party Comments
4	Illinois Municipal Electric Agency	Mary Ann Todd		None	N/A
4	Indiana Municipal Power Agency	Jack Alvey	Scott Berry	Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	LaGen	Richard Comeaux		Negative	Third-Party Comments
4	MGE Energy - Madison Gas and Electric Co.	Joseph DePoorter		Negative	Third-Party Comments
4	National Rural Electric Cooperative Association	Barry Lawson		Negative	Comments Submitted
4	North Carolina Electric Membership Corporation	John Lemire	Scott Brame	Negative	Third-Party Comments
4	Public Utility District No. 1 of Snohomish County	John Martinsen		Affirmative	N/A
4	Sacramento Municipal Utility District	Beth Tincher	Joe Tarantino	Affirmative	N/A
4	Seattle City Light	Hao Li		Negative	Comments Submitted
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho		Affirmative	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Abstain	N/A
4	WEC Energy Group, Inc.	Anthony Jankowski		Negative	Comments Submitted
5	Acciona Energy North America	George Brown		Negative	Comments Submitted
5	AEP	Thomas Foltz		Affirmative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Negative	Comments Submitted
5	APS - Arizona Public Service Co.	Kelsi Rigby		Affirmative	N/A
5	Arkansas Electric Cooperative Corporation	Moses Harris		Negative	Third-Party Comments
5	Associated Electric Cooperative, Inc.	Brad Haralson		None	N/A
5	Austin Energy	Shirley Mathew		None	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	Basin Electric Power Cooperative	Mike Kraft		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	BC Hydro and Power Authority	Helen Hamilton Harding		None	N/A
5	Berkshire Hathaway - NV Energy	Kevin Salsbury		Negative	Comments Submitted
5	Black Hills Corporation	George Tatar		Affirmative	N/A
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		Negative	Third-Party Comments
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	Brazos Electric Power Cooperative, Inc.	Shari Heino		Negative	Third-Party Comments
5	California Department of Water Resources	ASM Mostafa		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Negative	Third-Party Comments
5	City Water, Light and Power of Springfield, IL	Steve Rose		Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Negative	Comments Submitted
5	Colorado Springs Utilities	Jeff Icke		Affirmative	N/A
5	Dairyland Power Cooperative	Tommy Drea		None	N/A
5	Dominion - Dominion Resources, Inc.	Lou Oberski		Negative	Comments Submitted
5	DTE Energy - Detroit Edison Company	Jeffrey DePriest		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Negative	Comments Submitted
5	East Kentucky Power Cooperative	Steve Ricker		Affirmative	N/A
5	Entergy	Jamie Prater		Negative	Comments Submitted
5	Exelon	Ruth Miller		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	FirstEnergy - FirstEnergy Solutions	Robert Loy		Affirmative	N/A
5	Florida Municipal Power Agency	Chris Gowder	Brandon McCormick	Negative	Comments Submitted
5	Great Plains Energy - Kansas City Power and Light Co.	Harold Wyble	Douglas Webb	Affirmative	N/A
5	Great River Energy	Preston Walsh		Negative	Third-Party Comments
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	JEA	John Babik		None	N/A
5	Kissimmee Utility Authority	Mike Blough	Brandon McCormick	Negative	Comments Submitted
5	Lakeland Electric	Jim Howard		None	N/A
5	Lincoln Electric System	Kayleigh Wilkerson		Negative	Third-Party Comments
5	Manitoba Hydro	Yuguang Xiao		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	David Gordon		Negative	Third-Party Comments
5	MEAG Power	Steven Grego	Scott Miller	Abstain	N/A
5	Muscatine Power and Water	Neal Nelson		Negative	Third-Party Comments
5	NaturEner USA, LLC	Eric Smith		None	N/A
5	NB Power Corporation	Laura McLeod		Affirmative	N/A
5	Nebraska Public Power District	Don Schmit		Negative	Third-Party Comments
5	New York Power Authority	Erick Barrios		Negative	Third-Party Comments
5	NiSource - Northern Indiana Public Service Co.	Dmitriy Bazylyuk		Negative	Comments Submitted
5	North Carolina Electric Membership Corporation	Robert Beadle	Scott Brame	Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	OGE Energy - Oklahoma Gas and Electric Co.	John Rhea		Negative	Comments Submitted
5	Omaha Public Power District	Mahmood Safi		Negative	Third-Party Comments
5	Orlando Utilities Commission	Richard Kinas		None	N/A
5	OTP - Otter Tail Power Company	Cathy Fogale		Negative	Third-Party Comments
5	Platte River Power Authority	Tyson Archie		Affirmative	N/A
5	Portland General Electric Co.	Ryan Olson		Abstain	N/A
5	PPL - Louisville Gas and Electric Co.	JULIE HOSTRANDER		Affirmative	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Affirmative	N/A
5	Public Utility District No. 1 of Chelan County	Haley Sousa		Abstain	N/A
5	Public Utility District No. 1 of Pend Oreille County	Mark Cleveland		None	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Sacramento Municipal Utility District	Susan Oto	Joe Tarantino	Affirmative	N/A
5	Salt River Project	Kevin Nielsen		Negative	Third-Party Comments
5	Santee Cooper	Tommy Curtis		None	N/A
5	SCANA - South Carolina Electric and Gas Co.	Alyssa Hubbard		None	N/A
5	Southern Company - Southern Company Generation	William D. Shultz		Negative	Comments Submitted
5	Southern Indiana Gas and Electric Co.	Mark McDonald		Affirmative	N/A
5	SunPower	Bradley Collard		None	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Tennessee Valley Authority	M Lee Thomas		Affirmative	N/A
5	Tri-State G and T Association, Inc.	Mark Stein		Affirmative	N/A
5	U.S. Bureau of Reclamation	Wendy Center		Negative	Comments Submitted
5	WEC Energy Group, Inc.	Linda Horn		Negative	Comments Submitted
5	Xcel Energy, Inc.	Gerry Huitt		Affirmative	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Negative	Comments Submitted
6	APS - Arizona Public Service Co.	Jonathan Aragon		Affirmative	N/A
6	Arkansas Electric Cooperative Corporation	Bruce Walkup		Negative	Third-Party Comments
6	Associated Electric Cooperative, Inc.	Brian Ackermann		Negative	Comments Submitted
6	Basin Electric Power Cooperative	Paul Huettl		Negative	Third-Party Comments
6	Black Hills Corporation	Eric Scherr		None	N/A
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
6	Cleco Corporation	Robert Hirchak	Louis Guidry	None	N/A
6	Colorado Springs Utilities	Shannon Fair		Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Robert Winston		Negative	Comments Submitted
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
6	Duke Energy	Greg Cecil		Negative	Comments Submitted
6	Edison International - Southern California Edison Company	Kenya Streeter		Negative	Comments Submitted
6	Entergy	Julie Hall		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Exelon	Becky Webb		Negative	Comments Submitted
6	FirstEnergy - FirstEnergy Solutions	Ann Ivanc		Affirmative	N/A
6	Florida Municipal Power Agency	Richard Montgomery	Brandon McCormick	Negative	Comments Submitted
6	Florida Municipal Power Pool	Tom Reedy	Brandon McCormick	Negative	Comments Submitted
6	Great Plains Energy - Kansas City Power and Light Co.	Jennifer Flandermeyer	Douglas Webb	Affirmative	N/A
6	Great River Energy	Donna Stephenson	Michael Brytowski	Negative	Third-Party Comments
6	Los Angeles Department of Water and Power	Anton Vu		Affirmative	N/A
6	Manitoba Hydro	Blair Mukanik		None	N/A
6	Muscatine Power and Water	Ryan Streck	Amie Shuger McConnaha	Negative	Third-Party Comments
6	New York Power Authority	Shivaz Chopra	Shelly Dineen	Negative	Third-Party Comments
6	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joe O'Brien		Affirmative	N/A
6	Northern California Power Agency	Dennis Sismaet		Negative	Comments Submitted
6	NRG - NRG Energy, Inc.	Martin Sidor		None	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay		Negative	Third-Party Comments
6	Portland General Electric Co.	Daniel Mason		None	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
6	PSEG - PSEG Energy Resources and Trade LLC	Karla Barton		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Public Utility District No. 1 of Chelan County	Davis Jelusich		Abstain	N/A
6	Public Utility District No. 1 of Pend Oreille County	Kimberly Gentle		None	N/A
6	Public Utility District No. 2 of Grant County, Washington	LeRoy Patterson		None	N/A
6	Sacramento Municipal Utility District	Jamie Cutlip	Joe Tarantino	Affirmative	N/A
6	Salt River Project	Bobby Olsen		Negative	Third-Party Comments
6	Santee Cooper	Michael Brown		None	N/A
6	SCANA - South Carolina Electric and Gas Co.	John Folsom		None	N/A
6	Seattle City Light	Charles Freeman		Negative	Comments Submitted
6	Seminole Electric Cooperative, Inc.	Trudy Novak		Abstain	N/A
6	Snohomish County PUD No. 1	Franklin Lu		Affirmative	N/A
6	Southern Company - Southern Company Generation and Energy Marketing	Jennifer Sykes		Negative	Comments Submitted
6	Tacoma Public Utilities (Tacoma, WA)	Rick Applegate		Affirmative	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Affirmative	N/A
6	WEC Energy Group, Inc.	David Hathaway		Negative	Comments Submitted
6	Westar Energy	Megan Wagner		Affirmative	N/A
6	Western Area Power Administration	Charles Faust		Negative	Comments Submitted
6	Xcel Energy, Inc.	Carrie Dixon		Affirmative	N/A
8	David Kiguel	David Kiguel		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson		Negative	Third-Party Comments
10	Midwest Reliability Organization	Russel Mountjoy		Abstain	N/A
10	New York State Reliability Council	ALAN ADAMSON		Negative	Comments Submitted
10	Northeast Power Coordinating Council	Guy V. Zito		Negative	Comments Submitted
10	ReliabilityFirst	Anthony Jablonski		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Abstain	N/A

Previous 1 Next

Showing 1 to 298 of 298 entries

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2016-02 Modifications to CIP Standards

Formal Comment Periods Open through April 30, 2018
Ballot Pools Forming through April 16, 2018

Now Available

Three formal comment periods are open through **8 p.m. Eastern, Monday, April 30, 2018** for:

1. **CIP-002-6 – Cyber Security - BES Cyber System Categorization**
2. **CIP-012-1 – Cyber Security - Communications between Control Centers**
3. **Project 2016-02 Modifications to NERC Glossary of Terms Used in Reliability Standards – Control Center**

Commenting

Use the Standards Balloting and Commenting System (SBS) to submit comments. If you experience difficulties navigating the SBS, contact Wendy Muller. Unofficial Word versions of the comment forms are posted on the project page.

Ballot Pools

Ballot pools are being formed through **8 p.m. Eastern, Monday, April 16, 2018** for the **Control Center Definition** and its **Implementation Plan**. Registered Ballot Body members can join the ballot pools here.

- *If you are having difficulty accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out, contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern).*
- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*
- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Next Steps

The initial ballots for the **Control Center Definition** and its **Implementation Plan** will be conducted **April 20-30, 2018**. Additional ballots for **CIP-002-6** and **CIP-012-1** and the associated non-binding polls of the associated Violation Risk Factors and Violation Severity Levels will be conducted **April 20-30, 2018.**

For information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact Mat Bunch at (404) 446-9785 or Jordan Mallory at (404) 446-2589.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Comment Report

Project Name:	2016-02 Modifications to CIP Standards | Control Center Definition and Implementation Plan
Comment Period Start Date:	3/16/2018
Comment Period End Date:	4/30/2018
Associated Ballots:	2016-02 Modifications to CIP Standards Control Center Definition Implementation Plan IN 1 OT 2016-02 Modifications to CIP Standards Control Center Definition IN 1 DEF

There were 74 sets of responses, including comments from approximately 177 different people from approximately 127 companies representing 10 of the Industry Segments as shown in the table on the following pages.

Questions

1. Control Center definition: Do you agree with the proposed revisions to the definition of Control Center? If not, please provide rationale or propose an alternative definition.

2. Control Center definition: Do the proposed revisions to the Control Center definition change the scope or intent of any current or pending Reliability Standard(s) using the defined term (examples include Reliability Standards: COM-001-3; TOP-001-4; and IRO-002-5)? If yes, provide details of the affected Reliability Standard(s), requirements, and any anticipated impact.

3. Control Center definition: The SDT contends that there will be no change in BES Cyber System categorization by clarifying the definition of Control Center. This assertion is based on SDT review of the CIP-002-5.1a criteria and its understanding of BES Cyber System categorization through experience implementing CIP-002-5.1a. Do you agree with this assertion? If not, please provide rationale and practical examples of where a change in categorization will occur as a result of this modification.

4. Control Center definition: Is there a scenario where a Control Center hosts both the inclusion personnel and the exclusion personnel? If yes, please provide them here.

5. Implementation Plan: The new Control Center definition will become effective on the first day of the first calendar quarter that is three (3) calendar months after the effective date of the applicable governmental authority's order approving the term, or as otherwise provided for by the applicable governmental authority. Do you agree that three calendar months is enough time to update documentation? If you do not agree, please provide the amount of time needed and types of actions that will need to be completed during this time.

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim	3	RF	FirstEnergy Corporation	Aaron Ghdooshim	FirstEnergy - FirstEnergy Corporation	4	RF
					Aubrey Short	FirstEnergy - FirstEnergy Corporation	1	RF
					Theresa Ciancio	FirstEnergy - FirstEnergy Corporation	3	RF
					Robert Loy	FirstEnergy - FirstEnergy Solutions	5	RF
					Ann Ivanc	FirstEnergy - FirstEnergy Solutions	6	RF
Brandon McCormick	Brandon McCormick		FRCC	FMPA	Tim Beyrle	City of New Smyrna Beach Utilities Commission	4	FRCC
					Jim Howard	Lakeland Electric	5	FRCC
					Lynne Mila	City of Clewiston	4	FRCC
					Javier Cisneros	Fort Pierce Utilities Authority	3	FRCC
					Randy Hahn	Ocala Utility Services	3	FRCC
					Don Cuevas	Beaches Energy Services	1	FRCC
					Jeffrey Partington	Keys Energy Services	4	FRCC
					Tom Reedy	Florida Municipal Power Pool	6	FRCC
					Steven Lancaster	Beaches Energy Services	3	FRCC

					Mike Blough	Kissimmee Utility Authority	5	FRCC
					Chris Adkins	City of Leesburg	3	FRCC
					Ginny Beigel	City of Vero Beach	3	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
Seattle City Light	Ginette Lacasse	1,3,4,5,6	WECC	Seattle City Light Ballot Body	Pawel Krupa	Seattle City Light	1	WECC
					Hao Li	Seattle City Light	4	WECC
					Bud (Charles) Freeman	Seattle City Light	6	WECC
					Mike Haynes	Seattle City Light	5	WECC
					Michael Watkins	Seattle City Light	1,4	WECC
					Faz Kasraie	Seattle City Light	5	WECC
					John Clark	Seattle City Light	6	WECC
					Tuan Tran	Seattle City Light	3	WECC
					Laurrie Hammack	Seattle City Light	3	WECC
Entergy	Julie Hall	6		Entergy	Oliver Burke	Entergy - Entergy Services, Inc.	1	SERC
					Jamie Prater	Entergy	5	SERC
Southern Company - Southern Company Services, Inc.	Pamela Hunter	1,3,5,6	SERC	Southern Company	Katherine Prewitt	Southern Company Services, Inc.	1	SERC
					Joel Dembowski	Southern Company - Alabama Power Company	3	SERC

					William D. Shultz	Southern Company Generation	5	SERC
					Jennifer G. Sykes	Southern Company Generation and Energy Marketing	6	SERC
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,8,9,10	NPCC	RSC no Dominion, NextEra and HQ	Guy V. Zito	Northeast Power Coordinating Council	10	NPCC
					Randy MacDonald	New Brunswick Power	2	NPCC
					Wayne Sipperly	New York Power Authority	4	NPCC
					Glen Smith	Entergy Services	4	NPCC
					Brian Robinson	Utility Services	5	NPCC
					Alan Adamson	New York State Reliability Council	7	NPCC
					Edward Bedder	Orange & Rockland Utilities	1	NPCC
					David Burke	Orange & Rockland Utilities	3	NPCC
					Michele Tondalo	UI	1	NPCC
					Laura Mcleod	NB Power	1	NPCC
					David Ramkalawan	Ontario Power Generation Inc.	5	NPCC
					Helen Lainis	IESO	2	NPCC
					Michael Schiavone	National Grid	1	NPCC
					Michael Jones	National Grid	3	NPCC
					Michael Forte	Con Ed - Consolidated Edison	1	NPCC

					Peter Yost	Con Ed - Consolidated Edison Co. of New York	3	NPCC
					Sean Cavote	PSEG	4	NPCC
					Kathleen Goodman	ISO-NE	2	NPCC
					Paul Malozewski	Hydro One Networks, Inc.	3	NPCC
					Quintin Lee	Eversource Energy	1	NPCC
					Gregory Campoli	New York Independent System Operator	2	NPCC
					Dermot Smyth	Con Ed - Consolidated Edison Co. of New York	1,5	NPCC
					Dermot Smyth	Con Ed - Consolidated Edison Co. of New York	1,5	NPCC
					Salvatore Spagnolo	New York Power Authority	1	NPCC
					Shivaz Chopra	New York Power Authority	6	NPCC
					David Kiguel	Independent	NA - Not Applicable	NPCC
Midwest Reliability Organization	Russel Mountjoy	10		MRO NSRF	Joseph DePoorter	Madison Gas & Electric	3,4,5,6	MRO
					Larry Heckert	Alliant Energy	4	MRO
					Amy Casucelli	Xcel Energy	1,3,5,6	MRO
					Michael Brytowski	Great River Energy	1,3,5,6	MRO
					Jodi Jensen	Western Area Power Administratino	1,6	MRO
					Kayleigh Wilkerson	Lincoln Electric System	1,3,5,6	MRO
					Mahmood Safi	Omaha Public Power District	1,3,5,6	MRO

					Brad Parret	Minnesota Power	1,5	MRO
					Terry Harbour	MidAmerican Energy Company	1,3	MRO
					Tom Breene	Wisconsin Public Service	3,5,6	MRO
					Jeremy Volls	Basin Electric Power Coop	1	MRO
					Kevin Lyons	Central Iowa Power Cooperative	1	MRO
					Mike Morrow	Midcontinent Independent System Operator	2	MRO
Dominion - Dominion Resources, Inc.	Sean Bodkin	6		Dominion	Connie Lowe	Dominion - Dominion Resources, Inc.	3	NA - Not Applicable
					Lou Oberski	Dominion - Dominion Resources, Inc.	5	NA - Not Applicable
					Larry Nash	Dominion - Dominion Virginia Power	1	NA - Not Applicable
Southwest Power Pool, Inc. (RTO)	Shannon Mickens	2	SPP RE	SPP Standards Review Group	Shannon Mickens	Southwest Power Pool Inc.	2	SPP RE
					Steve Keller	Soutwest Power Pool Inc	2	SPP RE
					Sean Simpson	Board of Public Utilities, City of Mcpherson, Kansas	NA - Not Applicable	SPP RE
					louis Guidry	Cleco	1,3,5,6	SPP RE
Associated Electric Cooperative, Inc.	Todd Bennett	3		AECI	Michael Bax	Central Electric Power Cooperative (Missouri)	1	SERC
					Adam Weber	Central Electric Power	3	SERC

	Cooperative (Missouri)		
Stephen Pogue	M and A Electric Power Cooperative	3	SERC
William Price	M and A Electric Power Cooperative	1	SERC
Jeff Neas	Sho-Me Power Electric Cooperative	3	SERC
Peter Dawson	Sho-Me Power Electric Cooperative	1	SERC
Mark Ramsey	N.W. Electric Power Cooperative, Inc.	1	NPCC
John Stickley	NW Electric Power Cooperative, Inc.	3	SERC
Ted Hilmes	KAMO Electric Cooperative	3	SERC
Walter Kenyon	KAMO Electric Cooperative	1	SERC
Kevin White	Northeast Missouri Electric Power Cooperative	1	SERC
Skyler Wiegmann	Northeast Missouri Electric Power Cooperative	3	SERC
Ryan Ziegler	Associated Electric Cooperative, Inc.	1	SERC
Brian Ackermann	Associated Electric Cooperative, Inc.	6	SERC
Brad Haralson	Associated Electric Cooperative, Inc.	5	SERC

ACES Power Marketing	Warren Cross	1,3,4,5	MRO,RF,SERC,SPP RE,Texas RE,WECC	ACES Standards Collaborators	Arizona Electric Power Cooperative, Inc.	AEPC	1	WECC
					Hoosier Energy Rural Electric Cooperative, Inc.	HE	1	RF
					Rayburn Country Electric Cooperative	RCEC	3	SPP RE
					Southern Maryland Electric Cooperative	SMECO	3	RF
					North Carolina Electric Membership Corporation	NCEMC	3,4,5	SERC
					Central Iowa Power Cooperative	CIPCO	1	MRO
					East Kentucky Power Cooperative	EKPC	1,3	SERC
					Buckeye Power, Inc.	BUCK	4	RF
					Prairie Power, Inc.	PPI	1,3	SERC

1. Control Center definition: Do you agree with the proposed revisions to the definition of Control Center? If not, please provide rationale or propose an alternative definition.

Tony Eddleman - Nebraska Public Power District - 3	
Answer	No
Document Name	
Comment	

Trying to define a “control center” is difficult and can have unintended consequences. As you work your way through this definition, the boundary of a control center should be discussed and considered. Where is the boundary of a control center?

Reliability standard requirements contain words such as “within” a control center (TOP-001-4 R20), so the importance of knowing the boundary is important and in many cases, the boundary isn’t obvious. Control centers are typically located with other business functions and including a larger boundary than necessary can apply regulatory requirements to business functions not intended to be included in the requirement and introduce confusion. Possible boundaries may be defined by the following:

1. The property line or fence line of the facility. This broad brush of a definition will include functions not intended for applicability under Reliability Standards and cause unneeded costs for customers. In many cases where a control center is located in a metro area collocated in a building with other functions, a fence does not exist and the property line may be a public sidewalk. This definition is also problematic because cyber access equipment is not typically located at this boundary and access control would be extremely difficult. With the exception of a fence, gate, camera, etc., it is difficult to apply reliability controls to effectively control access with little ability to apply defense in-depth. Other concerns identified below for using the exterior building walls may also apply to using the property line or fence line. This definition is not recommended and should only be used in special cases.

2. The exterior building walls surrounding the control center. This definition is problematic due to other functions being collocated with the control center. If a control center is located with other business functions, such as a corporate headquarters, the control center may be located on a floor of a multiple floor building. In these situations, defining the exterior building walls is clearly an overextension of the regulatory requirements and will cause undue costs for an entity. Control centers may be collocated with a substation or power plant. For these situations, specific regulatory requirements may apply to the substation or power plant and simply designating the exterior building wall will confuse how to apply regulatory requirements. In a situation where you have a control center isolated from other business functions in a standalone facility, other support functions for the control center are needed. These support functions would not need the additional protections and will cause additional costs without a benefit to the BES. This definition may be used in specific situations, but should not be a default by everyone.

3. The Physical Security Perimeter (PSP) for the Control Center, or if a formal PSP is not required, the location where the PSP would be implemented, if required. A PSP is already defined in the NERC Glossary of Terms and entities have implemented security measures around these defined locations, where required. These are demarcations with clear boundaries and can be used to apply regulatory requirements. But, it’s easy to identify situations where identifying the boundary of a control center as a PSP may have unintended consequences. A PSP is defined for CIP requirements and trying to standardize by using a CIP term for an Operations & Planning requirement will lead to unintended consequences. A PSP is designed to contain BES Cyber Systems. In situations where you have multiple PSPs in the same building, you would need to address how the area between the PSPs is handled for the control center definition.

4. The boundary of a control center could be defined as the room(s) where NERC certified system operators perform real-time functions and the associated data centers. This definition limits the scope of the control center to the core functions and should provide a basis for the intent of the Reliability Standards. There may be exceptions, but this definition may cover a large percentage of registered entities that have a control center and need to identify a boundary.

Recommend the following definition:

One or more rooms in a facility, including their associated data centers, that monitor and control the Bulk Electric System (BES) and also host NERC certified operating personnel who:

Likes 2	Nebraska Public Power District, 5, Schmit Don; OGE Energy - Oklahoma Gas and Electric Co., 6, Tay Sing
Dislikes 0	

Response

Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1

Answer	No
Document Name	

Comment

POPUD is concerned that the proposed definition of Control Center may include Dispatching Centers (Distribution), Back-Up Centers and Power Plant Control Rooms in small utilities which have SCADA controls that control a very limited group of BES transmission assets. In our case, we provide SCADA to the various areas because of the multiple roles our staff has due to staffing constraints. We believe that the unintended consequences of the proposed change will impact us by confusing the auditing staff with the roles of Transmission Operators or Balancing Authorities; and, who must be NERC Certified. We own approximately 58 miles of transmission which is operated and monitored by another entity.

Likes 0	
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion

Answer	No
Document Name	

Comment

Dominion Energy disagrees with the proposed definition for the following reasons:

1. The term ‘real time reliability tasks’ is undefined and ambiguous. This term is critical to compliance and needs some additional context to allow entities to reliability operate. As such, there should be no obligations included in the task list for other Entities to perform. For example, one would not expect a TOP’s task list to require that a TO perform a task. Rather, the TOP may require that the TO identify a Real-time reliability task (in the TOs list under R2.1) to cover a situation. In this case, the real-time reliability-related task belongs to the TO and not the TOP. Consequently, one would never expect that a task be classified as real-time reliability-related for one Entity just because it has been designated as such by another Entity. For example, an RC may include running State Estimator and Contingency Analysis programs on its list of real-time reliability-related tasks. Just because a TO happens to run a State Estimator does not make running the State Estimator a real-time reliability-related task for the TO unless the TO has so designated it in the TO list, nor does the TO running the State Estimator satisfy the RC’s obligation to run the State Estimator.

2. If the context for ‘real time reliability tasks’ is PER-005, the task lists are entity specific and not necessarily shared with the entity responsible for determining if it’s a control center.

If PER-005 is the basis for these tasks, than the proposed Control Center definition should have the same language and limitations contained in PER-005.

1. Just because an entity performs a task on any RC, BA, TOP BES company-specific Real-time reliability-related task list, the proposed definition appears to automatically make that performance a reliability task that qualifies you as a Control Center.

If this is accurate, the responsible entity may not know what is on these lists as the entities that develop the lists are not required and, in most cases, do not share these with other entities.

1. As currently written, the proposed definition excludes the reliability related tasks developed by a TO and could make the TO fall under the definition of a Control Center unknowingly based on #3.

2. Based on ‘real time reliability tasks’ being defined in the context of PER-005, Dominion Energy proposes the following alternative language for a Control Center definition.

“One or more facilities, including their associated data centers, of an RC, BA, TOP, TO that monitor and control the Bulk Electric System (BES) and host operating personnel who can act independently to operate or direct in Real-time the operation of Bulk Electric System Transmission Facilities; or a centrally located GOP dispatch center hosting dispatch personnel at who receive direction from their RC, BA, TOP or TO and may develop specific dispatch instructions for plant operators or plant control systems under their control.

Operating and dispatch personnel do not include:

1. Transmission Owner or Transmission Operator field switching personnel; or

2. Plant operators located at a generator plant site or personnel at a centrally located dispatch center who relay dispatch instructions without making any modifications.

   The intent of the change to the definition is not clear in regards to TOs. Item 5 in the proposed definition of Control Center indicates that having the ability to operate a TO’s BES Transmission Facilities or merely having the ability to dispatch someone to operate the Facility creates a Control Center. Is the desired intent that any TO with SCADA control OR field switching personnel have a Control Center? Field switching personnel are excluded from the definition of “operating personnel”, but there is no definition of who is included in this definition. Is someone who answers the phone (e.g., from a TOP) and passes the instructions to field switching personnel considered to be “operating personnel”? Consider the example of a Storm Center (e.g., conference room) where personnel gather to monitor storm damage and direct field personnel for Real-time operation of the TO’s BES Transmission Facilities. Does the conference room become a Control Center under this definition, or is it excluded because those gathered in it are not considered operating personnel? This ambiguity should be resolved.

Likes 0	
Dislikes 0	

Response

Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF

Answer	No

Document Name	

Comment

Use of the term; “One or more facilities…” should be defined further as the NSRF believes the SDT’s intent and offer that a “facility” may be looked at as an entire building that houses RCs, BAs, and TOPs. Recommend that the first part of the definition read “One or more rooms in a facility…”. This clearly points to a prescribed area within a facility and not the entire facility.

Without understanding what “Real-time reliability-related tasks” are (see next paragraph), we cannot support this definition. There could be an entity that has personnel who work outside the “Control Center” walls that have Real-time tasks that support the RC, BA and TOP. Or is the SDT referring to NERC Certified System Operators only? Many entities require NERC Certifications for non-System Operators as part of the positions that they fulfill. Please clarify.

It is unclear to what the SDT believe the definition of “…reliability-related tasks…” refers to within is part 1, 2, and 3 of the proposed Control Center definition. Is this the “reliability-related tasks” associated with the tasks identified by each RC, TOP and BA per PER-005-2? Or is it the “reliability-related tasks” noted in some other NERC document? Note that “reliability-related tasks” is not used within the NERC Functional Model. The Functional Model uses “related reliability tasks”, only within the introduction sections and not under any specific Function. The term “Tasks” is used under each Function. Is the SDT referring to “Tasks” within the Functional Model to mean the same as “…reliability related tasks…” within the proposed Control Center definition? The NSRF is against using the Functional Model as a reference document as the current version is from 2010 and can be changed by NERC at any time. The NSRF recommends that an asterisk (*) [or foot note] be placed next to “reliability-related tasks*” and refer to reliability-related tasks identified by PER-005-2. This provides clarity the each applicable RC, TOP and BA.

Part 4 uses the word “can act” to describe the action that a GOP could accomplish in developing dispatch instructions. A GOP “can” do something but may not have the authority to accomplish the dispatch instruction. Recommend that part 4 use the word “perform” in place of “can act”, this is also in line with parts 1, 2, and 3.

Part 5 also uses the word “Can act”. Recommend this be replaced with “perform” with the same justification in part 4.

The NSRF would like to point out that the term "data center" is not defined in any NERC standard or NERC documentation. The issue is how far into the SCADA acquisition process does the data center definition penetrate. Does the data center definition penetrate into data aggregators used to reduce communication costs that represent loss of several RTU if compromised? The main impact area of this definition is in the new TOP-001-4 standard R20 that becomes enforceable 7-1-18. If the data center definition is beyond the bricks and mortar used for the Control Room and SCADA, then redundant
and diversely routed data exchange infrastructure may be needed outside of the traditional primary Control Center facility. Please clarify.

R20. Each Transmission Operator shall have data exchange capabilities, with redundant and diversely routed data exchange infrastructure within the Transmission Operator's primary Control Center, for the exchange of Real-time data with its Reliability Coordinator, Balancing Authority, and the entities it has identified it needs data from in order for it to perform its Real-time monitoring and Real-time Assessments.

Likes 2	OGE Energy - Oklahoma Gas and Electric Co., 6, Tay Sing; OGE Energy - Oklahoma Gas and Electric Co., 3, Hargrove Donald

Dislikes 0	

Response

Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	No
Document Name	2016-02_Control_Center_Modified_Definition_03162018-WECC comments.docx

Comment
Thank you for the opportunity to comment on the proposed revisions to the definition of Control Center. WECC agrees with and supports the purpose and intent of the proposed revisions to the Control Center Definition. WECC supports the revisions to the first five elements, and the concept behind the last two elements identifying what is not a control center. However, WECC believes that the definition of a Control Center should not include identifying what operating personnel are not, but rather, should include a definition of what a **Control Center** is not. WECC believes that including language defining what Operating personnel are not will conflict with the purpose of COM-002-4 – Operating Personnel Communications Protocols. There is evidence that a significant number of Misoperations are a result of poor communication between System Operators at control centers and the entity's operating personnel in the field. The attached file contains WECC's proposed revisions to the defintion.

Likes 0	
Dislikes 0	

Response

Jonathan Aragon - APS - Arizona Public Service Co. - 6	
Answer	No
Document Name	

Comment
a) For the purpose of clarity, AZPS recommends that the first sentence of the proposed definition be changed to: One or more facilities, including their associated data centers, hosting operating personnel that monitor and control the Bulk Electric System (BES) to: b) AZPS is concerned that the new definition sets up the potential for inconsistency due to the use of the term "reliability tasks" in the definition for items 1 and 3, but the term "functional obligations" in sections 1.1 and 1.3 of the CIP-002 attachment 1.   c) AZPS is concerned that item (5), which appears to be the equivalent of Transmission Operator Control Centers, presents a lower criteria for control centers than is applicable under item (3). Specifically, item 3, which is applicable to Transmission Operators, applies only when there are "facilities at two or more locations;" however, item 5, which could be construed as describing a Transmission Operator does not have the same qualifier. For this

reason, AZPS requests clarification of the use of “can operate” as stated in item 5 of the definition as well as what the intended differentiation between items 3 and 5 is.	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	No
Document Name	
Comment	
City Light supports APPA comments	
Likes 0	
Dislikes 0	
Response	
ALAN ADAMSON - New York State Reliability Council - 10	
Answer	No
Document Name	
Comment	
BES substation control rooms may be identified as “Control Centers” under the proposed definition; among other concerns, this could result in a substation being classified as High-Impact.	
Likes 0	
Dislikes 0	
Response	
Peter Yost - Con Ed - Consolidated Edison Co. of New York - 3	
Answer	No
Document Name	
Comment	
supporting comments from NPCC	

Likes 1	Central Hudson Gas & Electric Corp., 1, Pace Frank
Dislikes 0	

Response

Joel Charlebois - AESI - Acumen Engineered Solutions International Inc. - 5

Answer	No
Document Name	

Comment

With respect to Generator Operators and Generator Owners;

There are existing generation Facility control rooms, and perhaps other centralized control or data centers, who have the capability to operate or direct the operation of generation Facilities at two or more locations, but who do not develop specific dispatch instructions, but simply implement or relay (electronically in some cases) operating and dispatch instructions from their RC/BA/TOP, or from their GOP if the existing generation Facility control room implements or relays operating and dispatch instructions from a second larger GOP Control Center. These existing generation Facility control rooms meet the existing Control Center definition, but would be excluded from the proposed definition.

Some of these existing generation Facility control rooms can operate or direct the operation of Generator Owner Facilities at two or more locations (thereby meeting the existing Control Center definition) with an aggregate of 1500MW or more in a single Interconnection (e.g. 1000MW at one Facility, 500MW at another Facility), but simply implement or relay (electronically in some cases) operating and dispatch instructions from their RC/BA/TOP/GOP in doing so. The proposed definition will lower the impact rating of the BCS located at these exiting generation Facility control rooms from Medium under the CIP-002-5.1a impact rating criterion 2.11 down to Low under criterion 3.3, as these control rooms would no longer meet the proposed Control Center definition. The proposed Control Center definition adds new applicability criteria to CIP-002-5.1a impact rating criterion 2.11 by reference, thereby reducing the scope of applicability of CIP-002-5.1a impact rating criterion 2.11.

Since the intent of the CIP standards is to protect Cyber Assets and systems that “if rendered unavailable, degraded, or misused, would adversely impact the reliable operation of the BES within 15 minutes of the activation or exercise of the compromise”, the fact that a GOP (or GO) Facility’s control room operating personnel do or do not develop specific dispatch instructions for generation Facilities at two or more locations or simply implement or relay such instructions should be immaterial to the CIP-002-5.1a impact rating of the BCS located at those Facility control rooms.

As the 1500MW threshold is an important one and used in several CIP-002-5.1a Medium impact rating criteria, and the proposed definition will lower the impact rating of some BCS under CIP-002-5.1a impact rating criterion 2.11, we do not agree with the proposed definition.

We propose the following modifications:

1- Modify the sentence:

“4) can act independently as the Generator Operator to develop specific dispatch instructions for generation Facilities at two or more locations;”

To:

“4) act as the Generator Operator for generation Facilities at two or more locations;” which is similar to the existing definition, or perhaps to more accurately capture the intent of the CIP standards and to capture Facilities and control rooms performing GOP functions,

To:

“4) can operate or direct the operation of a Generator Owner’s BES generation Facilities at two or more locations in Real-time”, similar to the language of “5)”, which would capture all control rooms performing GOP functions for BES generation Facilities at two or more locations.

2- Remove exclusion “1) plant operators located at a generator plant site or personnel …”

Otherwise, CIP-002-5.1a impact rating criterion 2.11 should be modified to recapture Medium BCS at control centers or control rooms that would now be excluded from this criterion by the proposed definition.

With respect to Transmission Owner Control Centres (TOCCs);

The language in item “5)” should likely align with the concept in item “3)” with respect to operating or directing the operation of “Transmission Facilities at two or more locations;”

We propose the following modifications:

1- Modify the sentence:

“5) can operate or direct the operation of a Transmission Owner’s BES Transmission Facilities in Real-time.”

To:

“5) can operate or direct the operation of a Transmission Owner’s BES Transmission Facilities at two or more locations in Real-time.”

Likes 0	
Dislikes 0	

Response

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

BPA believes the majority of this definition isn’t needed. The only difference from existing System Operator definition being incorporated is the inclusion of GOP. BPA suggests using the defined term System Operator in the existing definition of Control Center and specifically including operating personnel at GOPs rather than listing all functions already covered in the current System Operator definition. The exclusions would also be covered in this manner since the System Operator definition only applies to people “at a Control Center.”

BPA proposes the following:

One or more facilities where the Bulk Electric System (BES) is monitored and controlled, including its associated data centers and communications infrastructure, and hosting operating personnel who:

1) perform the Real-time reliability-related tasks of a Reliability Coordinator; or

2) perform the Real-time reliability-related tasks of a Balancing Authority; or

3) perform the Real-time reliability-related tasks of a Transmission Operator for Transmission Facilities at two or more locations; or

4) can act independently as the Generator Operator to develop specific dispatch instructions for generation Facilities at two or more locations.

The exclusions aren't clear enough to know whether No. 1 only applies to personnel located at generating plants or includes personnel at other centrally located dispatch centers as well.

Operating personnel do not include:

1) Plant operators located at a generator plant site who relay or implement dispatch instructions from a Generator Operator without making any modifications; or

2) Personnel at a centrally located dispatch center who relay or implement dispatch instructions without making any modifications; or

3) Transmission Owner or Transmission Operator field switching personnel.

Likes 0	
Dislikes 0	

Response

Thomas Breene - WEC Energy Group, Inc. - 3

Answer	No
Document Name	

Comment

We support the MRO NSRF comments. The proposed definition of Control Center is fatally flawed in that it would allow for the exclusion of any data center which does not host operating personnel. This would introduce unacceptable security risks to the Bulk Electric System.

Likes 0	
Dislikes 0	

Response

Marty Hostler - Northern California Power Agency - 5,6

Answer	No
Document Name	

Comment

Agree with WECC's comments regarding specifying what a Control Center is not.

Also Attachment No. 1 item four is too ambiguous. "can act independently as the Generator Operator to develop specific dispatch instructions for generation Facilities at two or more locations". How does a GOP prove that they can not develop specific dispatch instructions?

I suggest the following: "Generator Operators that develop specific written dispatch instructions for generation Facilities, at two or more locations in real-time (at the same time), that deviate from their Balancing Authority's dispatch instructions".

Likes 0	
Dislikes 0	
Response	
Kenya Streeter - Edison International - Southern California Edison Company - 6	
Answer	No
Document Name	
Comment	
Please refer to comments submitted by Robert Blackney on behalf of Southern California Edison	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1	
Answer	No
Document Name	
Comment	
WAPA desires clarification on the definition of “associated data centers”. As written, it could bring data centers into scope that have nothing to do with power systems operations, but are “associated” in some other way. The qualifiers regarding “monitor and control the BES” and “host operating personnel” apply to the “One or more facilities” and not necessarily to “associated data centers”. As one example, there might be a business office data center that is associated with the facilities that monitor and host operating personnel. Another example might be that a scheduling vendor’s data center (which provides Net Scheduled Interchange data) is associated with the facilities that operate a Balancing Authority. More clarity is needed as to the intent in bringing “associated data centers” into this definition.	
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	

Duke Energy disagrees with the proposed revisions to the definition of Control Center based on the existence of some ambiguities. Regarding "operating personnel", is it the drafting team's intent that to be considered as operating personnel, does the personnel need to be able to control equipment such as opening a breaker? While we appreciate the drafting team's effort to provide more detail to explain who "operating personnel" actually applies to in the definition of Control Center, perhaps it may be more beneficial for operating personnel to have its own definition.

Also, the phrase "associated data centers", while already in use today, would benefit industry if a more common understanding was created. For example, is it the drafting team's intent that a facility would need to be manned to be considered applicable to this definition? Industry could benefit from having a common definition for "data center" as well.

Duke Energy offers the following suggested definition of Control Center for the drafting team's consideration:

One or more facilities, including their associated data centers for the acquisition, aggregation, processing, or inter-utility exchange of Bulk Electric System (BES) data that is used to support Real-time operations to make operational decisions regarding reliability and operability of the BES, and also host operating personnel, who monitor and control the BES and

1. perform the Real-time reliability-related tasks of a Reliability Coordinator; or Balancing Authority; or Transmission Operator for Transmission Facilities at two or more locations; or
2. can act independently as the Generator Operator to develop specific dispatch instructions for generation Facilities at two or more locations; or
3. can operate or direct the operation of a Transmission Owner's BES Transmission Facilities in Real-time.

Likes 0	
Dislikes 0	

Response

Douglas Johnson - American Transmission Company, LLC - 1

Answer	No
Document Name	

Comment

Operating personnel is vague and broad. American Transmission Company LLC (ATC) proposes replacing operating personnel with the NERC Glossary of Terms defined term System Operator. As a result, ATC requests consideration of rephrasing the first sentence as follows "One or more facilities, including their associated data centers, that monitor and control the Bulk Electric System (BES) and also host System Operators who:"

Likes 0	
Dislikes 0	

Response

Steven Mavis - Edison International - Southern California Edison Company - 1

Answer	No
Document Name	

Comment
Please refer to comments submitted by Robert Blackney on behalf of Southern California Edison

Likes 0	
Dislikes 0	

Response

Larry Watt - Lakeland Electric - 1	
Answer	No
Document Name	

Comment
1. The use of “host” in the first sentence is not understood. 2. The use of “including their associated data centers” in the proposed definition is a concern. Moving the “including their associated data centers” phrase as proposed, could suggest, to some, that the data center must host operating personnel. 3. The use of “perform the Real-time reliability related tasks of a” in Numbers 1-3 in the proposed definition is a concern. The additions of, “Real-time” and “related” to the existing “reliability tasks” does not provide additional clarity. These wording choices appear to be a reference to the NERC Functional Model, since the current Introduction to the Function Model (V5) includes subsections labeled “Tasks” and “Real Time.” An entity that performs the reliability tasks listed in the Functional Model should have the appropriate Functional Registration. For purposes of the Control Center definition, the three criteria should be limited to entities with the RC, BA and TOP registrations. Adding this phrase to points 1 -3 of the proposed definition does not address the issue of “capability or authority” as it relates to “perform.” Therefore, Lakeland Electric recommends striking this phrase in all locations. 4. Using “can” in point number 4 of the definition is a concern. Using “can” does not address the issue of “capability or authority.” Therefore, it is unclear how “can act” differs from the “perform” used in points 1-3. For example, if a VP of Operations for a GO (and not GOP) entity “can” order a unit shut to be shut down, would that entity’s facilities fit under the definition? Lakeland Electric recommends removing the word “can.” 5. Using “specific dispatch instructions” in definition point 4 is a concern. It is unclear how the addition of the word “specific” differentiates between different dispatch instructions. Therefore, Lakeland Electric recommends deleting the word “specific” and replacing the undefined “dispatch instructions” with the NERC defined term “Operating Instruction.” 6. The term “locations” used in point 4 is open to many interpretations and therefore causes concern. It is unclear how “locations” is applied to dispersed generation, adjoining or nested substations and switchyards. “Locations” may need to be defined in the NERC Glossary. 7. Use of “can” in the proposed definition point 5 causes concern. The word “can” does not address the issue of “capability or authority.” It is unclear how “can act” differs from the “perform” used in definition points 1-3. As written, this qualifier seems to go against the CIP-002-5.1 GTB (page 24) which states, “A TO BES Cyber System in a TO facility that does not perform or does not have an agreement with a TOP to perform any of these functional tasks does not meet the definition of a Control Center.” Therefore, Lakeland Electric recommends language that limits the scope to entities that have the capability. In addition, to ensure clarity, the GTB would need to be updated to agree with this change. 8. Use of, “Real-time” in point 5 without a pertinent understanding of how it will be specifically understood, causes concerns. The determination of how “Real-time” is applied was made by the SDT for the BES Cyber Asset definition developed under project 2014-02 Critical Infrastructure Protection Standards Version 5 Revisions - CIP-003, CIP-004, to mean “within 15 minutes of a required operation”. Lakeland Electric recommends that this 15-minute phrase be used in place of the “Real-time” term to ensure clarity.

9. Lakeland Electric believes the point 5 qualifier should use, “two or more locations,” to provide clarity to the proposed definition. Without this qualifying phrase, a facility at a TO with a single BES substation could be identified as a Control Center when “operating personnel” are present. Depending on how “host(ing)” is defined, all control buildings at a TO substation could be Control Centers under the proposed definition. APPA recommends adding the “two or more locations” phrase to this qualifying point 5.

10. Regarding exclusions with respect to operating personnel, point 1 states, “plant operators located at a generator plant site, or personnel at a centrally located dispatch center who….” It is unclear if both parts (plant operators~personnel) of this exclusion point, apply to only generation? The phrase, “generator plant site” can include both BES and non-BES generation and presents a lack of clarity. Public power recommends replacing “dispatch center” with “personnel who.” It is also possible for an operating instruction to be relayed for Transmission and not just Generation. Therefore, Lakeland Electric recommends removing the specific language limiting this exclusion to generation.

11. Exclusion point 1 includes, “dispatch instructions,” which is not a defined term. Lakeland Electic recommends replacing it with the NERC defined term “Operating Instruction.”

The suggestions above could result in the following definition:

One or more facilities that monitor and control the Bulk Electric System (BES) and host operating personnel during normal operations, including the facilities’ associated data centers, of a:

1) Reliability Coordinator; or

2) Balancing Authority; or

3) Transmission Operator for Transmission Facilities at two or more locations; or

4) Generator Operator that act independently to develop Operating Instructions for generation Facilities at two or more locations;

5) Generation Owner or Generation Operator that have generation Facilities that;

i) must operate, within 15 minutes of a required operation and

ii) are at two or more locations or

6) Transmission Owner that have the Transmission Facilities that:

i) must operate, within 15 minutes of a required operation and

ii) are at two or more locations or

Operating personnel do not include:

1) plant operators located at a generator plant site or personnel at a centrally located dispatch center who relay Operating Instructions without making any modifications; or

2) field switching personnel.

Likes 0	
Dislikes 0	

Response	
Julie Hall - Entergy - 6, Group Name Entergy	
Answer	No
Document Name	
Comment	

The NERC Rules of Procedure Section 500 and Appendix 5A require an entity which registers as a Balancing Authority (BA), Reliability Coordinator (RC), and Transmission Operator (TOP) to undergo Certification which requires an audit and readiness review of the registering entity to perform the functions of a BA, RC, or TOP. The control centers would have been identified under the program with exclusion to a GOP dispatcher for generation Facilities at two or more locations.

The current Control Center definition introduces the concept of a GOP Control Center and uses the undefined term “operating personnel.” The proposed Control Center definition creates potential conflict by overstating a control center function, attempting to define operating personnel, and uses the undefined term “plant operator.”

Recommend the following changes to the proposed Control Center definition and creation of an Operations Personnel definition.

Control Center - One or more facilities, including associated data centers, that hosts Operations Personnel who monitor, operate, or direct the operation of the Bulk Electric System (BES) in Real-time of: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for transmission Facilities at two or more locations, or 4) a Generator Operator’s generation Facilities at two or more locations.

Operations Personnel - Includes System Operators, Transmission Owner personnel, and centrally located dispatch personnel who develop specific dispatch instructions for Generator Operators under their control. The Transmission Owner or Transmission Operator personnel exclude field switching personnel. The dispatch personnel exclude Generator Operators who relay dispatch instructions without making any modifications.

Likes 0	
Dislikes 0	

Response	
Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	No
Document Name	
Comment	

NRECA strongly disagrees with the wording in item 5) of the proposed revised Control Center definition. As we have stated numerous times, a TO should not be considered to own/operate a Control Center unless they have the capability AND independent authority to operate BES Transmission Facilities in Real-time. NRECA recommends that item 5) be redrafted as follows: 5) can act with independent authority and capability to operate or direct the operation of a Transmission Owner’s BES Transmission Facilities in Real-time.

Likes 0	
Dislikes 0	

Response	
Chris Scanlon - Exelon - 1	
Answer	No
Document Name	
Comment	

Comment 1 - Exelon would like to see the following modification made to 5. :

5. can operate or direct the operation of a Transmission Owner's BES Transmission Facilities in Real-time, **at two or more locations**.

Without this additional language, Exelon is concerned that the current language in 5. may bring some currently out-of-scope relay houses into scope as Medium Control Centers.

Comment 2 - Exelon questions the wording of the first item under "Operating personnel do not include:" Exelon suggests the following wording change:

1. plant operators located at a generator plant site or personnel at a centrally located dispatch center who **can only** relay dispatch instructions and **cannot make any** modifications; or

This covers the situation where the normal process is for dispatch instructions to be relayed without modification, however, the system would allow the operating personnel to make modifications to the dispatch instructions.

Likes 0	
Dislikes 0	

Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	No
Document Name	
Comment	

The proposed changes to the definition do not address all of the "opportunities for clarification" and may add additional areas of uncertainty. Some of these issues are:

1) "host": Does this mean that a facility is a Control Center only when operating personnel are in the room? Example: A DP/TO with a two 115KV BES Substations staffs their emergency operations room during weather related emergency conditions. The facility can control the BES breakers at the BES substations. The facility is not staffed at most other times. Does this facility "host" operating personnel? Does this mean that a facility is a Control Center only when operating personnel are in the room? Adding the phrase "during normal operations" is meant to exclude locations like those mentioned in the example. We feel that this better defines a control center but may require that the list of assets in CIP-002 R1 be modified to include other assets. "Host" may need to be defined in the NERC Glossary.

2) “including their associated data centers”: Moving the “including their associated data centers” phrase, as proposed, could allow the interpretation that the data center must host operating personnel. Suggest restructuring this sentence. A suggested version of this language is included in the proposed definition included at the end of these comments.

3) Inclusion lines 1-3, “perform the Real-time reliability related tasks of a”: It is unclear how adding “Real-time” and “related” to the existing “reliability tasks” provides any clarity. This seems to be a direct reference to the NERC Functional Model. The Introduction to the Function Model (V5) as it includes subsections labeled “Tasks” and “Real Time.” An entity that performs the reliability tasks listed in the Functional Model should have the appropriate Functional Registration. These three criteria should be limited to entities with the RC, BA and TOP registrations. Adding this phrase to the inclusion lines 1 -3 does not address the issue of “capability or authority” as it relates to “perform”. Suggest striking this phrase in all locations.

4) Inclusion line 4, “can”: The word “can” phrase does not address the issue of “capability or authority”. It is unclear how “can act” differs from the “perform” used in lines 1-3. Does and entity meet this qualifier if a VP of Operations for a GO (and not GOP) entity can order that a unit shut down? Suggest removing the word “can”.

5) Inclusion line 4, “specific dispatch instructions”. It is unclear how the addition of the word “specific” differentiates between different dispatch instructions. Suggest deleting the word specific and replacing the undefined “dispatch instructions” with the NERC defined term “Operating Instruction”.

6) Inclusion line 4. This proposed definition does not include Generation that responds to Operating instructions for generation at two or more locations. Propose adding an inclusion that is similar to the inclusion criteria for Transmission Owners with Transmission Facilities at two or more locations.

7) Inclusion line 4, “locations”. The term “locations” is open to many interpretations. It is unclear how “locations” is applied to dispersed generation or adjoining or nested substations or switchyards. “Locations” may need to be defined in the NERC Glossary.

8) Inclusion line 5, “can”: The word “can” does not address the issue of “capability or authority”. It is unclear how “can act” differs from the “perform” used in lines 1-3. As written, this qualifier seems to go against the CIP-002-5.1 GTB (page 24) which states “A TO BES Cyber System in a TO facility that does not perform or does not have an agreement with a TOP to perform any of these functional tasks does not meet the definition of a Control Center.” Suggest replacing with language that limits the scope to entities that have the capability. The GTB would need to be updated to agree with this change.

9) Inclusion line 5, “Real-time”: The determination of how “Real-time” is applied was made by previous SDT to mean “within 15 minutes of a required operation”. Suggest that this 15-minute phrase be used in place of the “Real-time” term.

10) Inclusion line 5, “two or more locations”: This qualifier does not include the “two or more locations” phrase. Without this phrase, a facility at a TO with a single BES substation could be identified as a Control Center when “operating personnel” are present. Depending on how “hosting” is defined, all control buildings at a TO substation could be Control Centers. Suggest adding the “two or more locations” phrase to this qualifier.

11) Exclusions line 1, “plant operators located at a generator plant site or personnel at a centrally located dispatch center who”: It is unclear if both parts of this exclusion line applies to only generation. “generator plant site” would apply to both BES and non-BES generation. “Dispatch center” is undefined an could include the offices that dispatches service personnel. Suggest replacing the term with “personnel who”. It is also possible for an operating instruction to be relayed for Transmission and not just Generation. Suggest removing the specific language limiting this exclusion to generation.

12) Exclusion line 1, “dispatch instructions”. This term is undefined. Suggest replacing it with the NERC defined term “Operating Instruction”.

13) Change “Transmission Owner or Transmission Operator field switching personnel” to just “Field switching personnel” so that all field switching personnel are excluded.

The suggestions above could result in the following definition:

One or more facilities that monitor and control the Bulk Electric System (BES) and host operating personnel during normal operations, including the facilities’ associated data centers, of a:

1) Reliability Coordinator; or

2) Balancing Authority; or

3) Transmission Operator for Transmission Facilities at two or more locations; or

4) Generator Operator that act independently to develop Operating Instructions for generation Facilities at two or more locations;

5) Generation Owner or Generation Operator that monitor and control generation Facilities that;

i) must operate, within 15 minutes of an operation required by an Operating Instruction and

ii) are at two or more locations or

6) Transmission Owner that monitor and control Transmission Facilities that:

i) must operate, within 15 minutes of an operation required by an Operating Instruction and

ii) are at two or more locations or

Operating personnel do not include:

1) personnel who relay Operating Instructions without making modifications; or

2) field switching personnel.

Likes 0	
Dislikes 0	

Response

David Jendras - Ameren - Ameren Services - 3

Answer	No
Document Name	

Comment

- The term "operating personnel" should be changed to NERC defined term "System Operator".

- We believe the definition is overly complicated. Please consider the following wording to replace items 1-5:

A facility, including its associated data center(s), that houses equipment for the monitoring and control of the Bulk Electric System (BES) and also System Operators who must be trained in accordance with NERC Standard PER-005-2.

Rationale: FERC challenged NERC to identify those personnel whose job duties that have real-time reliability implications for BES reliability. As a response to the FERC directive, NERC established PER-005 to identify and govern those individuals who are RC, TOP, BA, TO, or GOP who have the real-time reliability tasks. On its face then, PER-005-2 identifies everyone whose work assets should be protected and also by exclusion those whose assets do not need to be protected since their work product does not affect real-time reliability (I.e. or else they should be trained.)

Likes 0	
Dislikes 0	

Response

Brandon McCormick - Brandon McCormick On Behalf of: Carol Chinn, Florida Municipal Power Agency, 6, 4, 3, 5; Chris Gowder, Florida Municipal Power Agency, 6, 4, 3, 5; David Owens, Gainesville Regional Utilities, 3, 1, 5; Ginny Beigel, City of Vero Beach, 3; Joe McKinney, Florida Municipal Power Agency, 6, 4, 3, 5; Mike Blough, Kissimmee Utility Authority, 5, 3; Richard Montgomery, Florida Municipal Power Agency, 6, 4, 3, 5; Tom Reedy, Florida Municipal Power Pool, 6; - Brandon McCormick, Group Name FMPA

Answer	No
Document Name	

Comment

FMPA agrees with the following comments from APPA:

APPA believes that the proposed Control Center definition needs to identify and address additional “opportunities for clarification.” Currently, the lack of clarity on these additional items increases uncertainty associated with the implementation of the proposed Control Center definition. “opportunities for clarification” include:

1. The use of “host” in the first sentence is not understood. Does this mean that a facility is a Control Center only when operating personnel are in the room? As an example:

a. An entity registered as a DP/TO with a two 115KV BES Substations staffs their emergency operations room during weather-related emergency conditions. Otherwise, the facility is not staffed. The facility can control the BES breakers at the BES substations.

Does the above scenario represent an instance that the facility is “host(ing)” operating personnel at the facility during emergencies? The proposed definition implies that a facility is a Control Center when operating personnel are (ever) in the room. APPA believes that adding the phrase, “host during normal operations” would provide the needed clarity. We believe that this change would improve the proposed Control Center definition. Public power recognizes that this change may require that the list of assets in CIP-002 R1 be modified to include other assets. Moreover, “host” may need to be defined in the NERC Glossary.

2. The use of “including their associated data centers” in the proposed definition is a concern. Moving the “including their associated data centers” phrase as proposed, could suggest, to some, that the data center must host operating personnel. Public power suggests restructuring this sentence. A suggested version of this language is included in the proposed definition provided at the end of these comments.

3. The use of “perform the Real-time reliability related tasks of a” in Numbers 1-3 in the proposed definition is a concern. The additions of, “Real-time” and “related” to the existing “reliability tasks” does not provide additional clarity. These wording choices appear to be a reference to the NERC Functional Model, since the current Introduction to the Function Model (V5) includes subsections labeled “Tasks” and “Real Time.” An entity that performs the reliability tasks listed in the Functional Model should have the appropriate Functional Registration. For purposes of the Control Center definition, the three criteria should be limited to entities with the RC, BA and TOP registrations. Adding this phrase to points 1 -3 of the proposed definition does not address the issue of “capability or authority” as it relates to “perform.” Therefore, APPA recommends striking this phrase in all locations.

4. Using “can” in point number 4 of the definition is a concern. Using “can” does not address the issue of “capability or authority.” Therefore, it is unclear how “can act” differs from the “perform” used in points 1-3. For example, if a VP of Operations for a GO (and not GOP) entity “can” order a unit shut to be shut down, would that entity’s facilities fit under the definition? APPA recommends removing the word “can.”

5. Using “specific dispatch instructions” in definition point 4 is a concern. It is unclear how the addition of the word “specific” differentiates between different dispatch instructions. Therefore, APPA recommends deleting the word “specific” and replacing the undefined “dispatch instructions” with the NERC defined term “Operating Instruction.”

6. The proposed definition’s point 4 does not include Generation that responds to operating instructions for generation at two or more locations. APPA proposes adding inclusion criteria for Generation, similar to the inclusion criteria for Transmission Owners with Transmission Facilities at two or more locations

7. The term “locations” used in point 4 is open to many interpretations and therefore causes concern. It is unclear how “locations” is applied to dispersed generation, adjoining or nested substations and switchyards. “Locations” may need to be defined in the NERC Glossary.

8. Use of “can” in the proposed definition point 5 causes concern. The word “can” does not address the issue of “capability or authority.” It is unclear how “can act” differs from the “perform” used in definition points 1-3. As written, this qualifier seems to go against the CIP-002-5.1 GTB (page 24) which states, “A TO BES Cyber System in a TO facility that does not perform or does not have an agreement with a TOP to perform any of these functional tasks does not meet the definition of a Control Center.” Therefore, APPA recommends language that limits the scope to entities that have the capability. In addition, to ensure clarity, the GTB would need to be updated to agree with this change.

9. Use of, “Real-time” in point 5 without a pertinent understanding of how it will be specifically understood, causes concerns. The determination of how “Real-time” is applied was made by the SDT for the BES Cyber Asset definition developed under project 2014-02 Critical Infrastructure Protection Standards Version 5 Revisions - CIP-003, CIP-004, to mean “within 15 minutes of a required operation”. APPA recommends that this 15-minute phrase be used in place of the “Real-time” term to ensure clarity.

10. APPA believes the point 5 qualifier should use, “two or more locations,” to provide clarity to the proposed definition. Without this qualifying phrase, a facility at a TO with a single BES substation could be identified as a Control Center when “operating personnel” are present. Depending on how “host(ing)” is defined, all control buildings at a TO substation could be Control Centers under the proposed definition. APPA recommends adding the “two or more locations” phrase to this qualifying point 5.

11. Regarding exclusions with respect to operating personnel, point 1 states, “plant operators located at a generator plant site, or personnel at a centrally located dispatch center who….” It is unclear if both parts (plant operators~personnel) of this exclusion point, apply to only generation? The phrase, “generator plant site” can include both BES and non-BES generation and presents a lack of clarity. Public power recommends replacing “dispatch center” with “personnel who.” It is also possible for an {C}1) operating instruction to be relayed for Transmission and not just Generation. Therefore, APPA recommends removing the specific language limiting this exclusion to generation.

12. Exclusion point 1 includes, “dispatch instructions,” which is not a defined term. Public power recommends replacing it with the NERC defined term “Operating Instruction.”

The suggestions above could result in the following definition:

One or more facilities that monitor and control the Bulk Electric System (BES) and host operating personnel during normal operations, including the facilities’ associated data centers, of a:

1) Reliability Coordinator; or

2) Balancing Authority; or

3) Transmission Operator for Transmission Facilities at two or more locations; or

4) Generator Operator that act independently to develop Operating Instructions for generation Facilities at two or more locations;

5) Generation Owner or Generation Operator that have generation Facilities that;

i) must operate, within 15 minutes of a required operation and

ii) are at two or more locations or

6) Transmission Owner that have the Transmission Facilities that:

i) must operate, within 15 minutes of a required operation and

ii) are at two or more locations or

Operating personnel do not include:

1) personnel who relay Operating Instructions without making modifications; or

2) field switching personnel.

Likes 0	
Dislikes 0	

Response

Dennis Sismaet - Northern California Power Agency - 6

Answer	No
Document Name	

Comment

Agree with WECC's comments regarding specifying what a Control Center is not.

Also Attachment No. 1 item four is too ambiguous. "can act independently as the Generator Operator to develop specific dispatch instructions for generation Facilities at two or more locations". How does a GOP prove that they can not develop specific dispatch instructions?

I suggest the following: "Generator Operators that develop specific written dispatch instructions for generation Facilities, at two or more locations in real-time (at the same time), that deviate from their Balancing Authority's dispatch instructions".

Likes 0	
Dislikes 0	

Response

Russell Noble - Cowlitz County PUD - 3,5

Answer	No
Document Name	

Comment

Cowlitz PUD supports the comments submitted by Brian Evans-Mongeon, Utility Services Inc.

Likes 0	
Dislikes 0	

Response

Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1

Answer	No
Document Name	

Comment

We support the following RSC comments :

- recommend changing "dispatching instructions" with the defined term "Operating instructions".
- Inclusion line 5 : "can" : The word “can” phrase does not address the issue of “capability or authority”. It is unclear how “can act” differs from the “perform” used in lines 1-3. As written, this qualifier seems to go against the CIP-002-5.1 GTB (page 24) which states “A TO BES Cyber System in a TO facility that does not perform or does not have an agreement with a TOP to perform any of these functional tasks does not meet the definition of a Control Center.” Recommend 1) replacing with language that limits the scope to entities that have the capability; 2) updating the GTB language to the new definition

- Inclusion line 5, “two or more locations”: This qualifier does not include the “two or more locations” phrase. Without this phrase, a facility at a TO with a single BES substation could be identified as a Control Center when “operating personnel” are present. Depending on how “hosting” is defined, all control buildings at a TO substation could be Control Centers. Recommend adding the “two or more locations” phrase to this qualifier.

- Exclusions line 1, “plant operators located at a generator plant site or personnel at a centrally located dispatch center who”: It is unclear if both parts of this exclusion line applies to only generation. “generator plant site” would apply to both BES and non-BES generation. “Dispatch center” is undefined and could include the offices that dispatches service personnel. Recommend replacing the “plant operators located at a generator plant site or personnel at a centrally located dispatch center who” with “personnel who”.

- Exclusion line 1, “dispatch instructions”. This term is undefined. Recommend replacing it with the NERC defined term “Operating Instruction”.

- Recommend removing Transmission Operator and Transmission Owner from the second exclusion, because Generator personnel can also perform field switching.

Our recommendations above could result in the following proposed definition:

One or more facilities, including their associated data centers, that monitor and control the Bulk Electric System (BES) and also host operating personnel who:

1. perform the Real-time reliability tasks of a Reliability Coordinator, or

2. perform the Real-time reliability tasks of a Balancing Authority; or

3. perform the Real-time reliability tasks of a Transmission Operator for Ttransmission Facilities at two or more locations;, or

4. has the capacity to act independently as the a Generator Operator to develop Operating instructions for generation Facilities at two or more locations; or.

5. has the capability to operate or direct the operation of a Transmission Owner's BES Transmission Facilities in Real-time at two or more locations.

Operating personnel do not include:

1) personnel who relay Operating Instructions without making modifications; or

2) field switching personnel.

Likes 0	
Dislikes 0	

Response

George Brown - Acciona Energy North America - 5

Answer	No
Document Name	

Comment

Supporting the MRO NSRF's comments.

Likes 0	
Dislikes 0	

Response

Heather Morgan - EDP Renewables North America LLC - 5

Answer	No
Document Name	

Comment

What does "Can act independently as the GOP" mean? Does "develop specific dispatch instructions" mean "develop specific dispatch instructions after receiving direction from the GOP's RC, BA, TOP, or TO"? There has been confusion within the generation industry on this meaning as evident in comments, questions, and concerns raised during the PER-005-2 project.

The current interpretation of the proposed definition as it relates to Generator Operators will impact not only NERC CIP Standards, but Operations and Planning Standards as well. With respect to CIP Standards, there are numerous generation control centers that do not develop specific dispatch instructions. Due to this, the proposed definition would impact the classification of BES Cyber Systems as required in CIP-002. Furthermore, generation

control centers with more than 1,500 MW in one or more Interconnection(s) would be able to easily revise operating protocols to ensure the entity never reaches the criteria to be classified as a Medium Impact BES Cyber Systems as defined with CIP-002. This loophole would not support the reliability of the Bulk Electric System.

EDPR NA advises the SDT to reconsider revising the definition of Control Center, which will have a significant impact on all NERC Standards, and include applicability segments to the desired standard similar to PER-005-2 rather than revising the definition of Control Center.

Likes 0	
Dislikes 0	

Response

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5

Answer	No
Document Name	

Comment

NV Energy believes that it is time to address the term “data centers” within the definition. If there is no defined NERC Glossary Term for a “data center”, the term becomes ambiguous, and interpretation is too subjective. NV Energy believes that NERC should address defining this term at this time.

NERC should provide further clarity within the revised definition, by adding the term “System Operator”, as the individuals perform the RT reliability tasks. This would better align with the expectation of the applicable parties/facilities that the NV Energy believes the definition is looking to address.

NV Energy identifies concerns with the Control Center definition and PER-005-2. The inclusion of “Real-Time reliability tasks” to the definition creates confusion between the standards. PER-005-2 identifies that Entities define their BES-company-specific RT reliability tasks, but the revised definition does not recognize that RT reliability tasks are Entity-specific. The definition should address that the RT reliability tasks performed at these locations, are defined by the Entity themselves, in order to better align with the existing PER-005-2 Standard.

NV Energy believes the use of passive action language as “…can act” is an issue. The inclusion of this language creates more questions than answers for defining Control Centers.

The exclusions section of the definition should also include a reference to Operations Support Personnel (i.e. IT and/or OT personnel), especially with inclusion of the PER-005-2 term, Real-time reliability tasks.

Likes 0	
Dislikes 0	

Response

Darnez Gresham - Darnez Gresham On Behalf of: Annette Johnston, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Darnez Gresham

Answer	No
Document Name	

Comment

We recommend the SDT consider approaches that correspond the scope of RC, TOP and BA Control Centers to the scope of EOP-008 and incorporate System Operator. We recommend considering qualifying draft criteria 1 (RC), 2 (BA) and 3 (TOP) with the concept of "System Operator." This aligns with the BES risk intended. We are concerned that EOP-008 appears absent in consideration of solutions for the definition with respect to RCs, TOPs and BAs. Yet, all EOP-008 versions since June 2007 have the stated purpose to continue reliable operations "in the event its control center becomes inoperable" and don't appear to have problems identifying the primary and backup control centers (Note: EOP-008 does not use the Glossary Control Center term). The Control Center definition has problematically created ambiguity since its origination, especially with the concept of "two or more locations." We also agree with MRO NSRF comments that "One or more facilities" should be reconsidered as well as "reliability related tasks."

In the GOP criteria (inclusion 4 and exclusion 1), following PER's words exactly is not working. For inclusion 4, "can act" and having the authority to act are not the same thing. See MRO NSRF comments. For exclusion 2, we reiterate comments from prior drafts that the PER concept of "plant operators located at a generator plant site" is antiquated and does not comprehend dispersed generation, including combustion turbines, wind and solar. Consider for exclusion 2, "personnel who do not independently make modifications to dispatch instructions for generation Facilities."

Inclusion 5 "can operate" is problematic. If a Transmission Owner can operate their Facilities at a substation (under the direction of a TOP) and not for switching, does inclusion 5 now make the substation a Control Center.

Additional exclusions are recommended to make it crystal clear that IT (information technology) and Operations Support Personnel are excluded.

We share concerns of other commenters on "data center" ambiguity. This includes other commenters concerns about how "and also host operating personnel" does or doesn't apply to data centers as currently drafted grammatically.

Likes 0	
Dislikes 0	

Response

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1

Answer	No
Document Name	

Comment

We recommend the SDT consider approaches that correspond the scope of RC, TOP and BA Control Centers to the scope of EOP-008 and incorporate System Operator. We recommend considering qualifying draft criteria 1 (RC), 2 (BA) and 3 (TOP) with the concept of "System Operator." This aligns with the BES risk intended. We are concerned that EOP-008 appears absent in consideration of solutions for the definition with respect to RCs, TOPs and BAs. Yet, all EOP-008 versions since June 2007 have the stated purpose to continue reliable operations "in the event its control center becomes inoperable" and don't appear to have problems identifying the primary and backup control centers (Note: EOP-008 does not use the Glossary Control Center term). The Control Center definition has problematically created ambiguity since its origination, especially with the concept of "two or more locations." We also agree with MRO NSRF comments that "One or more facilities" should be reconsidered as well as "reliability related tasks."

In the GOP criteria (inclusion 4 and exclusion 1), following PER's words exactly is not working. For inclusion 4, "can act" and having the authority to act are not the same thing. See MRO NSRF comments. For exclusion 2, we reiterate comments from prior drafts that the PER concept of "plant operators located at a generator plant site" is antiquated and does not comprehend dispersed generation, including combustion turbines, wind and solar. Consider for exclusion 2, "personnel who do not independently make modifications to dispatch instructions for generation Facilities."

Inclusion 5 “can operate” is problematic. If a Transmission Owner can operate their Facilities at a substation (under the direction of a TOP) and not for switching, does inclusion 5 now make the substation a Control Center.

Additional exclusions are recommended to make it crystal clear that IT (information technology) and Operations Support Personnel are excluded.

We share concerns of other commenters on “data center” ambiguity. This includes other commenters concerns about how “and also host operating personnel” does or doesn’t apply to data centers as currently drafted grammatically.

Likes 0	
Dislikes 0	

Response

Jack Cashin - American Public Power Association - 4

Answer	No
Document Name	

Comment

APPA believes that the proposed Control Center definition needs to identify and address additional “opportunities for clarification.” Currently, the lack of clarity on these additional items increases uncertainty associated with the implementation of the proposed Control Center definition. “opportunities for clarification” include:

1) The use of “host” in the first sentence is not understood. Does this mean that a facility is a Control Center only when operating personnel are in the room? As an example:

a. An entity registered as a DP/TO with a two 115KV BES Substations staffs their emergency operations room during weather-related emergency conditions. Otherwise, the facility is not staffed. The facility can control the BES breakers at the BES substations.

Does the above scenario represent an instance that the facility is “host(ing)” operating personnel at the facility during emergencies? The proposed definition implies that a facility is a Control Center when operating personnel are (ever) in the room. APPA believes that adding the phrase, “host during normal operations” would provide the needed clarity. We believe that this change would improve the proposed Control Center definition. Public power recognizes that this change may require that the list of assets in CIP-002 R1 be modified to include other assets. Moreover, “host” may need to be defined in the NERC Glossary.

2) The use of “including their associated data centers” in the proposed definition is a concern. Using the “including their associated data centers” phrase as proposed, could suggest, to some, that the data center must host operating personnel. Public power suggests restructuring this sentence. A suggested version of this language is included in the proposed definition provided at the end of these comments.

3) The use of “perform the Real-time reliability related tasks of a” in Numbers 1-3 in the proposed definition is a concern. The additions of, “Real-time” and “related” to the existing “reliability tasks” does not provide additional clarity. These wording choices appear to be a reference to the NERC Functional Model, since the current Introduction to the Function Model (V5) includes subsections labeled “Tasks” and “Real Time.” An entity that performs the reliability tasks listed in the Functional Model should have the appropriate Functional Registration. For purposes of the Control Center definition, the three criteria should be limited to entities with the RC, BA and TOP registrations. Adding this phrase to points 1 -3 of the proposed definition does not address the issue of “capability or authority” as it relates to “perform.” Therefore, APPA recommends striking this phrase.

4) Using “can” in point number 4 of the definition is a concern. Using “can” does not address the issue of “capability or authority.” Therefore, it is unclear how “can act” differs from the “perform” used in points 1-3. For example, if a VP of Operations for a GO (and not GOP) entity “can” order a unit shut to be shut down, would that entity’s facilities fit under the definition? APPA recommends removing the word “can.”

5) Using “specific dispatch instructions” in definition point 4 is a concern. It is unclear how the addition of the word “specific” differentiates between different dispatch instructions. Therefore, APPA recommends deleting the word “specific” and replacing the undefined “dispatch instructions” with the NERC defined term “Operating Instruction.”

6) The proposed definition’s point 4 does not include Generation that responds to operating instructions for generation at two or more locations. APPA proposes adding inclusion criteria for Generation, similar to the inclusion criteria for Transmission Owners with Transmission Facilities at two or more locations.

7) The term “locations” used in point 4 is open to many interpretations and therefore causes concern. It is unclear how “locations” is applied to dispersed generation, adjoining or nested substations and switchyards. “Locations” may need to be defined in the NERC Glossary.

8) Use of “can” in the proposed definition point 5 causes concern. The word “can” does not address the issue of “capability or authority.” It is unclear how “can act” differs from the “perform” used in definition points 1-3. As written, this qualifier seems to go against the CIP-002-5.1 GTB (page 24) which states, “A TO BES Cyber System in a TO facility that does not perform or does not have an agreement with a TOP to perform any of these functional tasks does not meet the definition of a Control Center.” Therefore, APPA recommends language that limits the scope to entities that specifically have the capability. In addition, to ensure clarity, the GTB would need to be updated to agree with this change.

9) Use of, “Real-time” in point 5 without a pertinent understanding of how it will be specifically understood, causes concerns. The determination of how “Real-time” is applied was made by the SDT for the BES Cyber Asset definition developed under project 2014-02 Critical Infrastructure Protection Standards Version 5 Revisions - CIP-003, CIP-004, to mean “within 15 minutes of a required operation”. APPA recommends that this 15-minute phrase be used in place of the “Real-time” term to ensure clarity.

10) APPA believes the point 5 qualifier should use, “two or more locations,” to provide clarity to the proposed definition. Without this qualifying phrase, a facility at a TO with a single BES substation could be identified as a Control Center when “operating personnel” are present. Depending on how “host(ing)” is defined, all control buildings at a TO substation could be Control Centers under the proposed definition. APPA recommends adding the “two or more locations” phrase to this qualifying point 5.

11) Regarding exclusions with respect to operating personnel, point 1 states, “plant operators located at a generator plant site, or personnel at a centrally located dispatch center who….” It is unclear if both parts (plant operators~personnel) of this exclusion point, apply to only generation? The phrase, “generator plant site” can include both BES and non-BES generation and presents a lack of clarity. Public power recommends replacing “dispatch center” with “personnel who.” It is also possible for an operating instruction to be relayed for Transmission and not just Generation. Therefore, APPA recommends removing the specific language limiting this exclusion to generation.

12) Exclusion point 1 includes, “dispatch instructions,” which is not a defined term. Public power recommends replacing it with the NERC defined term “Operating Instruction.”

The suggestions above could result in the following definition:

One or more facilities that monitor and control the Bulk Electric System (BES) and host operating personnel during normal operations, including the facilities’ associated data centers, of a:

1) Reliability Coordinator; or

2) Balancing Authority; or

3) Transmission Operator for Transmission Facilities at two or more locations; or

4) Generator Operator that act independently to develop Operating Instructions for generation Facilities at two or more locations;

5) Generation Owner or Generation Operator that monitor and control generation Facilities that;

i) must operate, within 15 minutes of an operation required by an Operating Instruction and

ii) are at two or more locations or

6) Transmission Owner that monitor and control the Transmission Facilities that:

i) must operate, within 15 minutes of an operation required by an Operating Instruction and

ii) are at two or more locations or

Operating personnel do not include:

1) personnel who relay Operating Instructions without making modifications; or

2) field switching personnel.	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	No
Document Name	
Comment	

Texas RE appreciates the opportunity to comment on the proposed revisions to the definition of a Control Center. While Texas RE appreciates the Standard Drafting Team's (SDT) efforts to develop a workable definition, Texas RE remains troubled regarding two aspects of the proposed revisions. First, Texas RE believes that the proposed revisions to the Generator Operator (GOP) Control Center definition are problematic and will lead to reliability gaps. Second, Texas RE contends that the use of the phrase "host operating personnel" could result in confusion among Registered Entities regarding the scope of their compliance obligations. Texas RE respectfully requests that the SDT remove these changes from the proposed definition. Alternatively, as detailed more fully below, the SDT must engage in a comprehensive review of the impact of these changes on all affective Reliability Standards and not simply focus on the proposed CIP-012 data exchange requirements.

As an initial matter, Texas RE is concerned that the proposed GOP Control Center definition improperly narrows the Control Center scope solely to GOP facilities that "can act independently . . . to develop specific dispatch instructions." In Texas RE's experience, a significant number of GOP entities have asserted that PER-005-2 is not applicable to their Control Centers due to language in that requirement limiting training obligations to circumstances in which GOP Control Center personnel act independently to develop specific dispatch instructions. Given this experience, Texas RE is concerned that the use of similar concepts of "independent operations" and "developing dispatch instructions" will result in a number of GOPs believing that their Control Centers are now largely excluded from the scope of the NERC CIP Cyber Security standards altogether. That is, the proposed definition implies that BES Cyber Systems located at significant centralized GOP control locations would longer meet the Medium or High Impact criteria in CIP-002-5.1a. As such, these BES Cyber Systems, despite potentially controlling thousands of MWs of generation resources potentially would not be required to possess the full range of physical and electronic protections specified throughout the NERC CIP Standards applicable to Medium and High Impact BES Cyber Systems.

Consider the following result. Under the current Control Center definition, BES Cyber Systems located at a "Control Center" performing the functional obligations of a GOP for generating units at a single plant location with an aggregate net Real Power capability equal to or exceeding 1500 MW in a single interconnection are current considered to be a High Impact BES Cyber Systems. Under the proposed Control Center definition, a GOP could reasonably conclude that because it only dispatches this 1500 MW Facility pursuant to the instructions from its Reliability Coordinator or Transmission Operator, it does not "independently" develop dispatch instructions. As such, the associated facility would no longer be a Control Center under the definition. Although the BES Cyber Systems at this facility are responsible for the control of a 1500 MW facility – identified by the Federal Energy Regulatory Commission (FERC) as the line at which the generation resource itself represents a heightened risk to reliability – the BES Cyber Systems at the facility actually controlling it would not need apply robust cyber security controls. This is wholly contrary to the intent underpinning the development of the CIP-002-5.1 impact rating criteria to provide clear "bright-line" criteria that is rooted in the actual impact an associated facility can have on the BES.

The SDT should decline to follow this approach. At a minimum, the Texas RE recommends the SDT fully evaluate this issue, develop a record, and provide FERC with information regarding the rationale for fundamentally redefining the CIP Standards in this manner.

In addition to these concerns, Texas RE also asserts that the proposed definition's use of the phrase "hosts operating personnel" is problematic. Texas RE asserts that the Control Center definitions above apply equally to primary and backup Control Centers. In Texas RE's reading, both types of facilities are capable of hosting operating personnel and, therefore, properly fall within the Control Center definition and all associated requirements. This reading makes sense from a reliability perspective, particularly given the expectation in EOP-008 that a backup Control Center will be capable of performing the same operating tasks as the primary Control Center for the duration of an issue at the primary facility. The proposed definition, however, potentially clouds this clear reliability picture. Specifically, entities could argue that only "hot" facilities actually "host operating personnel," and exclude backup Control Centers from the definition. This would be an erroneous reading of the definition. However, Texas RE suggests that the SDT add additional clarification by inserting the phrase "are capable of" so that the proposed definition reads "also are capable of hosting operating personnel" to clarify this issue.

Lastly, Texas RE is concerned that "Real-time reliability related tasks" is not defined. This will lead to each registered entity having its own criteria and not being consistent with the other entities performing the same function. It also may not include Operations Planning Analysis, which is just as important for reliable operations as Real-time analysis.

Likes 0	
Dislikes 0	

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6

Answer	No
Document Name	

Comment

Please see PacifiCorp's suggested edits to the definition below:

One or more facilities, including their associated data centers, that monitor and control the Bulk Electric System (BES) and also host operating personnel who:

1) are System Operators that perform the Real-time reliability-related tasks of a Reliability Coordinator; or

2) are System Operators that perform the Real-time reliability-related tasks of a Balancing Authority; or

3) are System Operators that perform the Real-time reliability-related tasks of a Transmission Operator for Transmission Facilities at two or more locations; or

4) are Generator Operator dispatch personnel at a centrally located dispatch center who receive direction from the Generator Operator's Reliability Coordinator, Balancing Authority, Transmission Operator, or Transmission Owner, and may develop specific dispatch instructions for plant operators under their control for generation Facilities at two or more locations; or

The current phrase " can act indepently as the Generator Operator to develop specific dispatch instructions" has been deleted from the proposed text above.

5) are Transmission Owner personnel who can act independently to operate or direct the operation of a Transmission Owner's BES Transmission Facilities in Real-time.

Operating personnel do not include:

1) are Generator Operator plant operators located at a generator plant site or personnel at a centrally located dispatch center who relay dispatch instructions without making any modifications; or

2) Transmission Owner or Transmission Operator field switching personnel.

3) Information Technology and Operational Technology personnel that perform task related to maintenance and security on BES Cyber Systems.

Adding System Operators to the scope of items 1, 2, & 3 narrows the scope sufficiently to include only the personnel trained and certified to operate the BES. The edits to item 4, along with exclusion 1, reflect the applicability from PER-005-2 for Generator Operators. However, we would like the Standards Drafting Team to address comments from prior drafts that the PER concept of "plant operators located at a generator plant site" is antiquated and does not comprehend dispersed generation, including combustion turbines, wind and solar, by making further changes to the exclusion or adding one for dispersed generation. The edits to item 5 reflect the applicability from PER-005-2 for Transmission Owner personnel. Adding an exclusion for Information Technology and Operational Technology personnel allows for them to perform their tasks related to their job descriptions without limiting the number of locations that they can be connected and communicating to at any given time, or inadvertently including them as operating personnel should they occupy a desk in a Control Center or associated data center. We share concerns of other commenters on "data center" ambiguity. This includes other commenters concerns about how "and also host operating personnel" does or doesn't apply to data centers as currently drafted grammatically.

Likes 0	
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	No
Document Name	

Comment

Southern Company would like to see clarification regarding the inclusion and exclusion statements where there are instances that a Generator Operator may partially meet an inclusion and exclusion at the same time. For example, a Generator Operator that does not "act independently" outside of its BA/RC, but that does develop specific dispatch instructions for non-reliability related functions may or may not be interpreted to be scoped in under this proposed definition. A Generator Operator may act independently to develop specific dispatch instructions that are relayed from a centrally located dispatch center to plant personnel (i.e., the GOP can monitor only – not monitor AND control), and may or may not be interpreted to be scoped in under this proposed definition. Additionally, if there is a facility that houses field switching personnel exclusively, and field switching is identified by a RC, BA and/or TOP as a "Real-time reliability-related task" in their PER-005-2 training programs, and the entity for which the field switching personnel are associated is registered as a RC, BA and/or TOP, then there is a conflict between the inclusions and exclusions.

Southern questions the use of "*Real-time reliability tasks"* in the scope of inclusions 1 through 3, but not in the scope of inclusions 4 and 5, and feels the term should be further defined. If the intent is an indirect reference to PER-005 *"Real-time reliability-related tasks"*, where applicability is to a Balancing Authority, Transmission Operator, Reliability Coordinator and Transmission Owner (even though the PER-005

applies to GOPs), this indirectly implies that the Generator Operator typically does not perform “Real-time reliability tasks”, therefore a specific exclusion to this effect is not warranted. This also appears to manifest itself in a change in wording for Inclusion Item 4 to “can act independently” in reference to the Generator Operator. The ability to act (i.e., “can”) is not equivalent to the authority to act. If the word “independently” included here is intended to suggest authority, then this remains ambiguous, at best. Southern feels that the definition of Control Center can be more clearly stated if more clarity is provided around what constitutes “Real-time reliability tasks”. For example, Southern suggests that to provide clarity the wording should be changed to: “GOPs that have been granted the authority by a BA, TOP or RC to make reliability decisions and incorporate these into their dispatch instructions.”

Southern also requests additional clarity be provided on the intent of the term “dispatch instructions” versus the NERC defined term “Operating Instructions.” We are not comfortable proceeding in support of this change without clarity on these terms and their use or omission from the proposed definition.

Additionally, Southern provides the following proposed definition of Control Center:

One or more facilities, including their associated data centers, that monitor and control the Bulk Electric System (BES) in Real-time and also hosts operating personnel that perform Real-time reliability-related tasks as defined and identified by the applicable Reliability Coordinator(s), Balancing Authority(ies), or Transmission Operator(s). Note: Real-time reliability-related tasks do not include the execution of Operating Instructions by Generator Operators as issued by applicable Reliability Coordinator(s), Balancing Authority(ies), or Transmission Operator(s).

*Note that the above definition does not require inclusions or exclusions. If there is a facility housing operating personnel under a Generator Operator registration and those operators monitor and control BES assets in real-time **and** perform Real-time reliability-related tasks defined and identified by their RC, BA or TOP, then the facility is a Control Center. If there is a facility that houses field switching personnel that monitor and control BES assets in real-time **and** perform Real-time reliability-related tasks defined and identified by their RC, BA or TOP, then the facility is a Control Center. If there is a facility that houses field switching personnel, but the facility does not allow for monitoring and control of BES assets in real-time, or does not perform Real-time reliability-related tasks defined and identified by their RC, BA or TOP, then the facility is not a Control Center.*

Likes 0	
Dislikes 0	

Response

Wendy Center - U.S. Bureau of Reclamation - 5

Answer	No
Document Name	

Comment

For all occurrences of the following terms, Reclamation recommends changing “Facilities” to “BES Facilities,” “Transmission Facilities” to “BES Transmission Facilities,” and “generation Facilities” to “BES generation Facilities” to reduce confusion. Therefore, first paragraph of the proposed definition should be revised to state:

“One or more BES facilities, including their associated Data Centers, that monitor and control the BES and also host System Operators who...”

and items 3 and 4 of the proposed definition should be revised as follows:

- perform the Real-time reliability-related tasks of a Transmission Operator for any BES Transmission Facilities; or

- can act independently as the Generator Operator to develop specific dispatch instructions for any BES generation Facilities.

Reclamation also recommends adding the following definitions to the NERC Glossary of Terms:

- Data Center: A location used to interchange BES Data.
- BES Data: BES reliability operating services information affecting Operational Planning Analysis, Real-time Assessments, and Real-time monitoring.

Likes 0	
Dislikes 0	

Response

Warren Cross - ACES Power Marketing - 1,3,4,5 - MRO,Texas RE,SERC,SPP RE,RF, Group Name ACES Standards Collaborators

Answer	No
Document Name	

Comment

1. ACES supports the standard drafting team (SDT) and NERC efforts to clarify the definition of a Control Center. However, ACES suggests the SDT use NERC-defined terms that have been industry vetted and/or defined in the NERC Glossary of Terms, and those terms used consistently. Examples of terms that are vague, overly broad, and/or not NERC-defined include “operating personnel”, “Real-time reliability tasks”, “monitor and control” (does the ability to “monitor” belong in the definition at all?), and “2 or more locations.”

2. ACES requests further clarification regarding Line (5) regarding operation of a Transmission Owner’s BES Transmission Facilities in Real-time to eliminate any confusion by small entities operating under a TOP’s jurisdictional control. ACES suggests the following alternative language:

5) “acts independently to operate or direct the operation of a Transmission Owner’s BES Transmission Facilities in Real-time.”

3. As proposed, the Control Center definition seems to be encompassing all entities with BES Facilities, regardless of size or impact to the BES. From a cyber-security standpoint, we understand that a cyber attacker is not going to ask permission from a TOP before performing actions on the BES, and that NERC is trying to address that risk. However, aren’t those risks and mitigations addressed in the Low Impact CIP Requirements? Is it NERC’s intent to pull virtually every control center and associated data center into scope? Many small entities (with no material impact to the BES) would be brought in under the proposed definition.

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion, NextEra and HQ	
Answer	No
Document Name	
Comment	

The proposed changes to the definition do not address all of the “opportunities for clarification” and may add additional areas of uncertainty. Some of these issues are:

1) Inclusion lines 1-3, Recommend striking “perform the Real-time reliability related tasks of a:” this phrase in all locations. It is unclear how adding “Real-time” and “related” to the existing “reliability tasks” provides any clarity. This seems to be a direct reference to the NERC Functional Model. The Introduction to the Function Model (V5) as it includes subsections labeled “Tasks” and “Real Time”. An entity that performs the reliability tasks listed in the Functional Model should have the appropriate Functional Registration. Adding this phrase to the inclusion lines 1 -3 does not address the issue of “capability or authority” as it relates to “perform”. Inclusions line 1-3 should only apply to Entity with those Functional Registrations

2) Inclusion line 4, “can act independently”: The word “can” phrase does not address the issue of “capability or authority”. It is unclear how “can act” differs from the “perform” used in lines 1-3. Does an entity meet this qualifier if a VP of Operations for a GO (and not GOP) entity can order that a unit shut down? Recommend removing the word “can”.

3) Inclusion line 4, “specific dispatch instructions”. It is unclear how the addition of the word “specific” differentiates between different dispatch instructions. Recommend replacing the undefined “dispatch instructions” with the NERC defined term “Operating Instruction”.

4) Inclusion line 5, “can”: The word “can” phrase does not address the issue of “capability or authority”. It is unclear how “can act” differs from the “perform” used in lines 1-3. As written, this qualifier seems to go against the CIP-002-5.1 GTB (page 24) which states “A TO BES Cyber System in a TO facility that does not perform or does not have an agreement with a TOP to perform any of these functional tasks does not meet the definition of a Control Center.” Recommend 1) replacing with language that limits the scope to entities that have the capability; 2) updating the GTB language to the new definition

5) Inclusion line 5, “two or more locations”: This qualifier does not include the “two or more locations” phrase. Without this phrase, a facility at a TO with a single BES substation could be identified as a Control Center when “operating personnel” are present. Depending on how “hosting” is defined, all control buildings at a TO substation could be Control Centers. Recommend adding the “two or more locations” phrase to this qualifier.

6) Exclusions line 1, “plant operators located at a generator plant site or personnel at a centrally located dispatch center who”: It is unclear if both parts of this exclusion line applies to only generation. “generator plant site” would apply to both BES and non-BES generation. “Dispatch center” is undefined and could include the offices that dispatches service personnel. Recommend replacing the “plant operators located at a generator plant site or personnel at a centrally located dispatch center who” with “personnel who”.

7) Exclusion line 1, “dispatch instructions”. This term is undefined. Recommend replacing it with the NERC defined term “Operating Instruction”.

8) Recommend removing Transmission Operator and Transmission Owner from the second exclusion, because Generator personnel can also perform field switching.

The recommendations above could result in the following definition:

One or more facilities that monitor and control the Bulk Electric System (BES) and host operating personnel, including the facilities' associated data centers, of a:

1) Reliability Coordinator; or

2) Balancing Authority; or

3) Transmission Operator for Transmission Facilities at two or more locations; or

4) Generator Operator that act independently to develop Operating Instructions for generation Facilities at two or more locations; or

5) Transmission Owner that have the capability to operate, in Real-time, the Transmission Owner's Transmission Facilities, at two or more locations.

Operating personnel do not include:

1) personnel who relay Operating Instructions without making modifications; or

2) field switching personnel.

Likes 0	
Dislikes 0	

Response

David Ramkalawan - Ontario Power Generation Inc. - 5

Answer	No
Document Name	

Comment

Line 4, by adding the requirement that it must have the capability "to develop specific dispatch instructions", excludes facilities that are currently included and traditionally considered to be control centers. In the case where dispatches are received and modified or developed at a central "control center" facility and sent to regional control centers who act on but do not modify those dispatches, those regional control centers would seem to no longer be control centers by the proposed definition when, in fact, that is where the most sensitive, directly controlling systems (such as SCADA) reside. These regional control centers often directly control remote, unstaffed generation Facilities directly through their BCS. A viable GOP control center definition must consider the differences between control centers that merely co-ordinate and issue instructions (dispatches) and control centers that

directly control generating resources, such as those that have BCS that remotely control normally unstaffed generation Facilities. If both types are intended to be included, the defining criteria must be common to both or distinguish between and specifically apply to each type.

Proposal for Line 4: a) who develop or modify dispatch instructions that are sent to either another control center or 2 or more generation facilities or b) who have the potential to supply the final authoritative human supplied control inputs at least some of the time for 2 or more generation facilities.

Note that the suggested Line 4 above eliminates the need for Exclusion Line 1. The wording of b) would likely need to be refined, but the idea is to capture the people who have the ability to input control inputs to operate generating resources without the need for other people's involvement. For example, a remote operator at a "control center" that can control the remote resource without the need for local personnel at the remote generation resource to intercede. The existence of local operators or local control capability does not interfere with criteria b).

Line 4 - Dispatch instruction is not a defined term – suggest using the term operational instruction.

Likes 0	
Dislikes 0	

Response

Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 3

Answer	No
Document Name	

Comment

PNM disagrees with the proposed revision to the definition of Control Center. We agree with concerns about the use of "real-time reliability tasks" as raised by Dominion Energy, EEI, and Texas RE. We also share WECC's concern that "including language defining what Operating personnel are not will conflict with the purpose of COM-002-4 – Operating Personnel Communications Protocols." We also share Texas RE's concern that "that BES Cyber Systems located at significant centralized GOP control locations would longer meet the Medium or High Impact criteria."

Thus we recommend to either 1) change the criteria in CIP-002 Attachment 1 Impact Rating Criteria to achieve the desired outcome of scoping out smaller facilities, or 2) consider Entergy's recommended definition of Control Center and proposed term Operations Personnel.

Likes 0	
Dislikes 0	

Response

Laurie Williams - PNM Resources - Public Service Company of New Mexico - 1

Answer	No
Document Name	

Comment	
Concur with PNM-Lynn Goldstein Comments	
Likes 0	
Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	No
Document Name	
Comment	
The phrase “act independently” could be interpreted to exclude current Control Centers that act solely on direction of the ISO. NRG believes the intent to be has the ability to control rather than act independently. NRG recommends that the verbiage be clarified. The first exception lists plant operators at a generating plant site. This implies that plant control rooms that have the ability to start or monitor units at other plant locations would not be considered Control Centers. NRG recommends that this should be clarified.	
Likes 0	
Dislikes 0	
Response	
Faz Kasraie - Seattle City Light - 5 - WECC	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
Answer	No
Document Name	
Comment	

Likes 0	
Dislikes 0	

Response

Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino

Answer	Yes
Document Name	

Comment

References to Real – time should be consistent with the NERC Glossary.

Likes 0	
Dislikes 0	

Response

Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE

Answer	Yes
Document Name	

Comment

While Xcel Energy generally agrees with the proposed revisions, there is some concern with the lack of clarity in the verbiage in items #4 and #5. We note the exception of operating personnel identified in #1 and #2 of the "Operating personnel do not include" section. However, additional clarity provided would resolve cencerns. Xcel Energy suggests editing the language to read:

4) Has the authority to act independently as the Generator Operator to develop specific dispatch instructions for generation Facilities at two or more locations; or

5) Has the authority to operate or direct the operation of a Transmission Owner's BES Transmission Facilities in Real-time.

Likes 0	
Dislikes 0	

Response

Teresa Cantwell - Lower Colorado River Authority - 1,5

Answer	Yes
Document Name	
Comment	
No comments.	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	Yes
Document Name	
Comment	
The SPP Standards Review Team suggests that the drafting team takes into consideration, providing some clarification for the lower case term facilities. The defined term of Facility in the Glossary of terms focuses on electrical equipment serving as a single BES Element. However, there is some confusion on what the lower case term facilities are applicable to. During our discussions, there were questions of could the term be referring to a specific room in a building or is it an entire building? From our perspective, this clarity is needed to help the industry get a better understanding to meet the expectations of the definition which helps ensure the reliability of the grid. Additionally, we would suggest revising to #4 and #5 in the definition to read as follows: 4. Can have the authority to act independently as the Generator Operator to develop specific dispatch instructions for generation Facilities at two or more locations; or 5. Has the authority act independently to operate or direct the operation of a Transmission Owner's BES Transmission Facilities in Real-time.	
Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Consider the following revision: "(4) can act independently as the Generator Operator to develop specific dispatch instructions for generation Facilities at two or more locations that have the ability to impact the BES;"	

Likes 0	
Dislikes 0	
Response	
Linda Jacobson-Quinn - City of Farmington - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sandra Pacheco - Silicon Valley Power - City of Santa Clara - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Val Ridad - Silicon Valley Power - City of Santa Clara - 3,4,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeff Ipsaro - Silicon Valley Power - City of Santa Clara - 3,4,5	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Maier - Intermountain REA - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kristine Ward - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
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	
Aaron Austin - AEP - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 1	CMS Energy - Consumers Energy Company, 4, Martinez Theresa
Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8,9 - WECC	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1,3,5 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 3, Group Name FirstEnergy Corporation	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Stephanie Burns - Stephanie Burns On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Stephanie Burns	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ellen Oswald - Midcontinent ISO, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Anderson - CMS Energy - Consumers Energy Company - 1	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrey Komissarov - Sempra - San Diego Gas and Electric - 7 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dmitriy Bazylyuk - NiSource - Northern Indiana Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	
Document Name	
Comment	
AECI supports comments provided by NRECA	
Likes 0	
Dislikes 0	
Response	

2. Control Center definition: Do the proposed revisions to the Control Center definition change the scope or intent of any current or pending Reliability Standard(s) using the defined term (examples include Reliability Standards: COM-001-3; TOP-001-4; and IRO-002-5)? If yes, provide details of the affected Reliability Standard(s), requirements, and any anticipated impact.

Warren Cross - ACES Power Marketing - 1,3,4,5 - MRO,Texas RE,SERC,SPP RE,RF, Group Name ACES Standards Collaborators

Answer	No
Document Name	

Comment

No comments.

Likes 0	
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	No
Document Name	

Comment

The term “control center” is used in other Standards as an undefined term (lower case “c”s). Specifically, in COM-001-3, referenced in Requirements R12 and R13, which apply to the GOP and DP functions, respectively. Both requirements specify that Interpersonal Communication capability is required “between control centers within the same functional entity, and/or between a control center and field personnel.” [Note that “control center” is lower case (i.e., an undefined term)]. Southern does not believe that the proposed Control Center definition change is in conflict with the Requirements of COM-001-3, but the term “control cent

In TOP-001-4, the context in these Requirements R20, R21, and R24 refer C definition of Control Center does not create any concerns or conflicts provided that applicability for these Requirements is not expanded to other functions such as GOPs because they are explicitly included in the new definition of Control Center.

In IRO-002-5, the context in these Requirements R2 and R3 refers to the proposed definition of “ Control Center does not create any concerns or conflicts provided that the applicability for these Requirements is not expanded to other functions such as GOPs because they are explicitly included in the new definition of Control Center.

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	No

Document Name	
Comment	
The definition of Control Center has changed substantively. Texas RE has identified 40 standard requirements that contain the term control center (upper and lowercase). Texas RE inquires as to whether the SDT analyzed all of these requirements in order to determine the implications of the revised definition of Control Center on other standards.	
Likes 0	
Dislikes 0	
Response	
Jack Cashin - American Public Power Association - 4	
Answer	No
Document Name	
Comment	
COM-001-3 requires internal Interpersonal Communication capabilities between Control Centers and field personnel. It is unclear if the proposed Control Center definition revision could be interpreted to also require these capabilities to and from the “associated data center” (the phrase used in the current definition of Control Center. While this concern does not seem to be caused by changes in the proposed definition, clarity is needed. Possibly this could be clarified in COM-001 guidance.	
Likes 0	
Dislikes 0	
Response	
Russell Noble - Cowlitz County PUD - 3,5	
Answer	No
Document Name	
Comment	
Cowlitz PUD supports the comments submitted by Brian Evans-Mongeon, Utility Services Inc.	
Likes 0	
Dislikes 0	
Response	
Brandon McCormick - Brandon McCormick On Behalf of: Carol Chinn, Florida Municipal Power Agency, 6, 4, 3, 5; Chris Gowder, Florida Municipal Power Agency, 6, 4, 3, 5; David Owens, Gainesville Regional Utilities, 3, 1, 5; Ginny Beigel, City of Vero Beach, 3; Joe McKinney,	

Florida Municipal Power Agency, 6, 4, 3, 5; Mike Blough, Kissimmee Utility Authority, 5, 3; Richard Montgomery, Florida Municipal Power Agency, 6, 4, 3, 5; Tom Reedy, Florida Municipal Power Pool, 6; - Brandon McCormick, Group Name FMPA	
Answer	No
Document Name	
Comment	
FMPA agrees with the following comments from APPA: COM-001-3 requires internal Interpersonal Communication capabilities between Control Centers and field personnel. It is unclear if the proposed Control Center definition revision could be interpreted to also require these capabilities to and from the “associated data center” (the phrase used in the current definition of Control Center. While this concern does not seem to be caused by changes in the proposed definition, clarity is needed. Possibly this could be clarified in COM-001 guidance.	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	No
Document Name	
Comment	
COM-001-3 requires internal Interpersonal Communication capabilities between Control Centers and field personnel. It is unclear if this revision could be interpreted to require these capabilities to and from the associated data center. (The “associated data center” phrase is in the existing definition of Control Center. This concern does not seem to be caused by changes in the proposed definition.) This may need to be clarified in guidance to COM-001.	
Likes 0	
Dislikes 0	
Response	
Larry Watt - Lakeland Electric - 1	
Answer	No
Document Name	
Comment	
COM-001-3 requires internal Interpersonal Communication capabilities between Control Centers and field personnel. It is unclear if the proposed Control Center definition revision could be interpreted to also require these capabilities to and from the “associated data center” (the phrase used in the	

current definition of Control Center. While this concern does not seem to be caused by changes in the proposed definition, clarity is needed. Possibly this could be clarified in COM-001 guidance.	
Likes 0	
Dislikes 0	
Response	
Kenya Streeter - Edison International - Southern California Edison Company - 6	
Answer	No
Document Name	
Comment	
Please refer to comments submitted by Robert Blackney on behalf of Southern California Edison	
Likes 0	
Dislikes 0	
Response	
Thomas Breene - WEC Energy Group, Inc. - 3	
Answer	No
Document Name	
Comment	
We support the MRO NSRF comments.	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
None	

Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	No
Document Name	
Comment	
City Light supports SRP comments	
Likes 0	
Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ellen Oswald - Midcontinent ISO, Inc. - 2	
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	

Stephanie Burns - Stephanie Burns On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Stephanie Burns	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Douglas Johnson - 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	
Adrian Andreoiu - BC Hydro and Power Authority - 1,3,5 - WECC	
Answer	No
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Faz Kasraie - Seattle City Light - 5 - WECC	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jonathan Aragon - APS - Arizona Public Service Co. - 6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Austin - AEP - 3,5	
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	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Kristine Ward - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Maier - Intermountain REA - 3	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeff Ipsaro - Silicon Valley Power - City of Santa Clara - 3,4,5	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Val Ridad - Silicon Valley Power - City of Santa Clara - 3,4,5	

Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sandra Pacheco - Silicon Valley Power - City of Santa Clara - 5	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 3	
Answer	Yes
Document Name	
Comment	
PNM believes that COM-001-3 is the one most likely to be affected since it is the only one with Generation Operator Control Centers in scope and that is what the definition is trying to change.	
Likes 0	
Dislikes 0	
Response	
David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	

CIP-012 and CIP-002. Facilities that are considered GOP control centers would no longer be if they do not host people who originate or modify dispatch instructions.

Likes 0	
Dislikes 0	

Response

Wendy Center - U.S. Bureau of Reclamation - 5

Answer	Yes
Document Name	

Comment

If Reclamation's proposed revisions are adopted, changes to the scope of COM-001-3 could be interpreted. To avoid changing the scope of COM-001-3, Reclamation recommends modifying COM-001-3 to replace "Control Center" with "primary Control Center" throughout the Reliability Standard to align COM-001-3 with TOP-001-4 and IRO-002-5.

Likes 0	
Dislikes 0	

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6

Answer	Yes
Document Name	

Comment

PacifiCorp supports MEC's comments regarding TOP-001-4: The main impact area of this definition is in the new TOP-001-4 standard R20 that becomes enforceable 7-1-18. If the data center definition is beyond the bricks and mortar used for the Control Room and SCADA, then redundant and diversely routed data exchange infrastructure may be needed outside of the traditional primary Control Center facility. R.20. says: "R20. Each Transmission Operator shall have data exchange capabilities, with redundant and diversely routed data exchange infrastructure within the Transmission Operator's primary Control Center, for the exchange of Real-time data with its Reliability Coordinator, Balancing Authority, and the entities it has identified it needs data from in order for it to perform its Real-time monitoring and Real-time Assessments." Please provide additional clarity.

Likes 0	
Dislikes 0	

Response

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1

Answer	Yes
Document Name	

Comment

We support that EOP-008-2 (future enforceable) and prior versions do NOT (and should not) use the Control Center definition, but rather apply to “control centers” for RCs, TOPs and BAs. We are not aware of plans to change that. However, Control Center first only existed in CIP standards and has since crept into non-CIP standards. It is important that the definition revision consider what would happen to other standards, such as EOP-008, if future revisions of EOP-008 considered adopting “Control Center” to replace “control center.”

The main impact area of this definition is in the new TOP-001-4 standard R20 that becomes enforceable 7-1-18. If the data center definition is beyond the bricks and mortar used for the Control Room and SCADA, then redundant and diversely routed data exchange infrastructure may be needed outside of the traditional primary Control Center facility. R.20. says: “R20. Each Transmission Operator shall have data exchange capabilities, with redundant and diversely routed data exchange infrastructure within the Transmission Operator's primary Control Center, for the exchange of Real-time data with its Reliability Coordinator, Balancing Authority, and the entities it has identified it needs data from in order for it to perform its Real-time monitoring and Real-time Assessments.” Please clarify.

Likes 0	
Dislikes 0	

Response

Darnez Gresham - Darnez Gresham On Behalf of: Annette Johnston, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Darnez Gresham

Answer	Yes
Document Name	

Comment

We support that EOP-008-2 (future enforceable) and prior versions do NOT (and should not) use the Control Center definition, but rather apply to “control centers” for RCs, TOPs and BAs. We are not aware of plans to change that. However, Control Center first only existed in CIP standards and has since crept into non-CIP standards. It is important that the definition revision consider what would happen to other standards, such as EOP-008, if future revisions of EOP-008 considered adopting “Control Center” to replace “control center.”

The main impact area of this definition is in the new TOP-001-4 standard R20 that becomes enforceable 7-1-18. If the data center definition is beyond the bricks and mortar used for the Control Room and SCADA, then redundant and diversely routed data exchange infrastructure may be needed outside of the traditional primary Control Center facility. R.20. says: “R20. Each Transmission Operator shall have data exchange capabilities, with redundant and diversely routed data exchange infrastructure within the Transmission Operator's primary Control Center, for the exchange of Real-time data with its Reliability Coordinator, Balancing Authority, and the entities it has identified it needs data from in order for it to perform its Real-time monitoring and Real-time Assessments.” Please clarify.

Likes 0	
Dislikes 0	

Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
The current and revised Control Center definition is actually presently impacting interpretation for TOP-001-4, Requirement 20. Without an official definition for a data center, interpretation of the Control Center perimeter (per this Standard), may require redundant and diversely routed data exchange infrastructure to be required outside of the traditional primary Control Center facility.	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5	
Answer	Yes
Document Name	
Comment	
No comments.	
Likes 0	
Dislikes 0	
Response	
Heather Morgan - EDP Renewables North America LLC - 5	
Answer	Yes
Document Name	
Comment	
The NERC SDT should consider the impact on COM-001-3. With the proposed definition, many generation Control Centers (as currently defined within the NERC Glossary) would no longer be a Control Center (with the proposed definition). With the proposed definition, many current Generator Operator Control Centers would not have to have Interpersonal Communication “between Control Centers within the same functional entity, and/or between a Control Center and field personnel” since they do not develop specific dispatch instructions as proposed.	

Likes 0	
Dislikes 0	
Response	
George Brown - Acciona Energy North America - 5	
Answer	Yes
Document Name	
Comment	
Supporting the MRO NSRF's comments.	
Likes 0	
Dislikes 0	
Response	
Dmitriy Bazylyuk - NiSource - Northern Indiana Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Within this proposed definition it appears that the SDT is interpreting who should *not* be included as "operating personnel". Is this just in the context of the Control Center definition or throughout the NERC Standards? For example would this apply to COM-002-4 Operating Personnel Communication Protocols R1 R2 R3 R4? Maybe "operating personnel" should be defined separately. **Also, in addition to standards mentioned in this question, this proposed definition is tied to other definitions such as "Operating Instruction" and "System Operator". This may change the "scope or intent" of Reliability Standards which would require further review.**	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	

(Ditto EEI Comments):

- COM-001-3; One scenario may be a GO could direct (verbally or through automatic schemes) a TO Facility to operate in support of a RAS.
- COM-001-3: The proposed Control Center definition excludes field switching personnel. COM-001-3 R12 uses the Control Center definition and includes communications between Control Centers and field personnel. Do the words of the Standard over-ride the proposed definition? The proposed Control Center definition is in conflict with COM-001-3, R12 and will lead to uncertainty with CEAs and Applicable Entities.
- IRO-002-5 uses the phrase "…and other entities deemed necessary…" which allows the RC to be added any entity to the RC's Monitoring and Analysis capabilities. No issue.
- TOP-001-4 (effective 7/1/2018); This Standard's Applicability section may need to be expanded if there are entities identified per the proposed Control Center definition, such as a GO who can direct a Transmission Facility to do something to save their generator (RAS).
- IRO-002 and TOP-001 both use the terms "primary" Control Centers in each of their applicable Requirement language. COM-001-3 uses the term Control Center. Does the proposed definition include both primary and secondary Control Centers? If so, request that the SDT make this statement for all Applicable Entities to understand.

Likes 0	
Dislikes 0	

Response

Chris Scanlon - Exelon - 1

Answer	Yes
Document Name	

Comment

Yes the definition may change scope or intent of these standards, unless the added phrase "at two or more locations" is added to 5.

Likes 0	
Dislikes 0	

Response

Barry Lawson - National Rural Electric Cooperative Association - 4

Answer	Yes
Document Name	

Comment

Additional impacted standards include EOP-004-4 and EOP-008-1. To the extent the Control Center definition is revised and moves forward, it is possible that new Control Centers will be identified or a Control Center impact rating could increase. Because of this, the proposed Implementation Plan should be revised to provide additional time for non-CIP standard compliance impacted by the revised Control Center definition.

Likes 0	
Dislikes 0	

Response

Julie Hall - Entergy - 6, Group Name Entergy

Answer	Yes
Document Name	

Comment

Please see comments for Question 4.

Likes 0	
Dislikes 0	

Response

sean erickson - Western Area Power Administration - 1

Answer	Yes
Document Name	

Comment

WAPA is in agreement with the comment that the term "data center" is not defined in any NERC standard or NERC documentation. The issue is how far into the SCADA acquisition process does the data center definition penetrate. Does the data center definition penetrate into data aggregators used to reduce communication costs that represent loss of several RTU if compromised? The main impact area of this definition is in the new TOP-001-4 standard R20 that becomes enforceable 7-1-18. If the data center definition is beyond the bricks and mortar used for the Control Room and SCADA, then redundant and diversely routed data exchange infrastructure may be needed outside of the traditional primary Control Center facility. Please clarify.

Likes 0	
Dislikes 0	

Response

Steven Rueckert - Western Electricity Coordinating Council - 10

Answer	Yes

Document Name	
Comment	

COM-002-4

Concern that proposed definition would cause uncertainty in whether or not personnel at control centers must use three part communications. There is evidence that a significant number of Misoperations are a result of poor communication between System Operators at control centers and the entity's operating personnel in the field.

Likes 0	
Dislikes 0	
Response	

Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF

Answer	Yes
Document Name	
Comment	

COM-001-3; One scenario may be a GO could direct (verbally or through automatic schemes) a TO Facility to operate in support of a RAS.

COM-001-3: The proposed Control Center definition excludes field switching personnel. COM-001-3 R12 uses the Control Center definition and includes communications between Control Centers and field personnel. Do the words of the Standard over-ride the proposed definition? The proposed Control Center definition is in conflict with COM-001-3, R12 and will lead to uncertainty with CEAs and Applicable Entities.

IRO-002-5 uses the phrase "…and other entities deemed necessary…" which allows the RC to added any entity to the RC's Monitoring and Analysis capabilities. No issue.

TOP-001-4 (effective 7/1/2018); This Standard's Applicability section may need to be expanded if there are entities identified per the proposed Control Center definition, such as a GO who can direct a Transmission Facility to do something to save their generator (RAS).

IRO-002 and TOP-001 both use the terms "primary" Control Centers in each of their applicable Requirement language. COM-001-3 uses the term Control Center. Does the proposed definition include both primary and secondary Control Centers? If so, request that the SDT make this statement for all Applicable Entities to understand.

Likes 1	OGE Energy - Oklahoma Gas and Electric Co., 3, Hargrove Donald
Dislikes 0	
Response	

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion

Answer	Yes
Document Name	
Comment	

The impacts to the non CIP Standards have not been examined at length due to the abbreviated amount of time available, but many non-CIP standards rely on the definition of Control Center.

Likes 0	
Dislikes 0	

Response

Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1

Answer	Yes
Document Name	

Comment

There is no choice for potentially. The unintended consequences will not be known until the auditing of standards has begun after the definition change. The auditors, who are responsible to measure compliance performance, can have a subjective change in interpretation for applicability of many standards. It is the duty of the Drafting Team to make a complete analysis of the existing standards to assure there is not misapplication due to the change in definition.

Likes 0	
Dislikes 0	

Response

Dennis Sismaet - Northern California Power Agency - 6

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Andrey Komissarov - Sempra - San Diego Gas and Electric - 7 - WECC

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 3, Group Name FirstEnergy Corporation	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Marty Hostler - Northern California Power Agency - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8,9 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Linda Jacobson-Quinn - City of Farmington - 3	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	
Document Name	
Comment	
AECI supports comments provided by NRECA	
Likes 0	
Dislikes 0	
Response	
Joel Charlebois - AESI - Acumen Engineered Solutions International Inc. - 5	
Answer	
Document Name	
Comment	
Yes. CIP-002-5.1a impact rating criterion 2.11. See response to question #1.	
Likes 0	
Dislikes 0	
Response	
Tony Eddleman - Nebraska Public Power District - 3	
Answer	
Document Name	
Comment	

COM-001-3: The proposed Control Center definition excludes field switching personnel. COM-001-3 R12 uses the Control Center definition and includes communications between Control Centers and field personnel. This is a Conflict with the proposed definition of Control Center.

IRO-002 and TOP-001 both use the terms “primary” Control Centers in each of their applicable Requirement language. COM-001-3 uses the term Control Center. When one looks at proposed CIP-012-1 it is apparent in the rationale section of the Implementation Guide that Backup Control Centers are included. Can one assume that “Control Center” used in Reliability Standards includes the Backup Control Center? Will this result in consistent appication?

Likes 1	Nebraska Public Power District, 5, Schmit Don
Dislikes 0	

Response

3. Control Center definition: The SDT contends that there will be no change in BES Cyber System categorization by clarifying the definition of Control Center. This assertion is based on SDT review of the CIP-002-5.1a criteria and its understanding of BES Cyber System categorization through experience implementing CIP-002-5.1a. Do you agree with this assertion? If not, please provide rationale and practical examples of where a change in categorization will occur as a result of this modification.

Tony Eddleman - Nebraska Public Power District - 3

Answer	No
Document Name	

Comment

Without knowing the boundary of a control center as discussed above in question one, it is not possible to answer this question. Will the new definition of a control center, without a boundary as currently written, produce unintended consequences of bringing new cyber assets into CIP compliance? At a minimum, a larger than required control center will require CIP-002 screening for BES Cyber Systems to include countless systems not intended to be screened for entities collocated with other business functions.

Likes 1	Nebraska Public Power District, 5, Schmit Don
Dislikes 0	

Response

Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1

Answer	No
Document Name	

Comment

Dispatch centers of small utilities that are not categorized as Control Centers will now fall under that category. They will be categorized as low impact facilities. It is possible that some plant control rooms will also be considered as Control Centers now because they may be responsible for local and remote generation, or generation that is within the same campus, but not the same facility. Some large industrial sites, with their own generation, fall under this category.

Likes 0	
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion

Answer	No
Document Name	

Comment

It is unclear if entities with facilities not previously defined as a Control Center will now be considered a Control Center, resulting in newly categorized BES Cyber Systems.	
Likes 0	
Dislikes 0	
Response	
Kenya Streeter - Edison International - Southern California Edison Company - 6	
Answer	No
Document Name	
Comment	
Please refer to comments submitted by Robert Blackney on behalf of Southern California Edison	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1	
Answer	No
Document Name	
Comment	
It is possible that the ambiguity of the language “associated data center” could result in an unintended consequence within BES Cyber System categorization.	
Likes 0	
Dislikes 0	
Response	
Stephanie Burns - Stephanie Burns On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Stephanie Burns	
Answer	No
Document Name	
Comment	

Language on inclusion 5 includes “direct operations” which is too vague for clear interpretation.

Likes 0	
Dislikes 0	

Response

Barry Lawson - National Rural Electric Cooperative Association - 4

Answer	No
Document Name	

Comment

There are an unknown number of scenarios where the BES Cyber System impact rating/categorization could be impacted. Because of the potential impacts to non-CIP standards, the proposed Implementation Plan should be revised to provide additional time for non-CIP standard compliance impacted by the revised Control Center definition.

Likes 0	
Dislikes 0	

Response

David Jendras - Ameren - Ameren Services - 3

Answer	No
Document Name	

Comment

Clarification needs to be added around "associated data center" and whether it is included due to its relationship in support the Control Center or because it contains operating personnel/System Operators (obviously, the former).

Likes 0	
Dislikes 0	

Response

George Brown - Acciona Energy North America - 5

Answer	No
Document Name	

Comment

From a Generator Operator perspective the proposed definition of Control Center does not.

Likes 0	
Dislikes 0	

Response

Heather Morgan - EDP Renewables North America LLC - 5

Answer	No
Document Name	

Comment

The current interpretation of the proposed definition as it relates to Generator Operators will impact not only NERC CIP Standards, but Operations and Planning Standards as well. With respect to CIP Standards, there are numerous generation control centers that do not develop specific dispatch instructions. Due to this, the proposed definition would impact the classification of BES Cyber Systems as required in CIP-002. Furthermore, generation control centers with more than 1,500 MW in one or more Interconnection(s) would be able to easily revise operating protocols to ensure the entity never reaches the criteria to be classified as a Medium Impact BES Cyber Systems as defined with CIP-002. This loophole would not support the reliability of the Bulk Electric System.

Furthermore, current Low Impact BES Cyber System Control Centers that do not “develop specific dispatch instructions,” will no longer have a Low Impact BES Cyber System Control Center with the proposed changes.

Likes 0	
Dislikes 0	

Response

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5

Answer	No
Document Name	

Comment

NV Energy does not recognize an impact for its facilities, but the fact that additional criteria have been added to define a Control Center, there is an opportunity than an Entity will now have facilities that were not previously identified as a Control Center, now in scope of the Impact Criterion.

Likes 0	
Dislikes 0	

Response

Darnez Gresham - Darnez Gresham On Behalf of: Annette Johnston, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Darnez Gresham	
Answer	No
Document Name	
Comment	
We have had confidence on what in version 5 are our high and medium impact Control Centers. Depending on the revised Control Center definition, low impact Control Centers could be in doubt. Refer to concerns with the definition.	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	
Comment	
We have had confidence on what in version 5 are our high and medium impact Control Centers. Depending on the revised Control Center definition, low impact Control Centers could be in doubt. Refer to concerns with the definition.	
Likes 0	
Dislikes 0	
Response	
Warren Cross - ACES Power Marketing - 1,3,4,5 - MRO,Texas RE,SERC,SPP RE,RF, Group Name ACES Standards Collaborators	
Answer	No
Document Name	
Comment	
It does not change the criteria used in CIP-00205.1a but it does influence the entity if they are now ruled a Control Center. If so, then that new Control Center should have time to reevaluate their BES Cyber System categorization process and update their documentation.	
Likes 0	
Dislikes 0	
Response	

Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	No
Document Name	
Comment	
Please see NRG comment to Question number 1.	
Likes 0	
Dislikes 0	
Response	
Faz Kasraie - Seattle City Light - 5 - WECC	
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	
Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
Answer	No
Document Name	
Comment	

Likes 0	
Dislikes 0	

Response

Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body

Answer	Yes
Document Name	

Comment

City Light supports SRP comments

Likes 0	
Dislikes 0	

Response

Peter Yost - Con Ed - Consolidated Edison Co. of New York - 3

Answer	Yes
Document Name	

Comment

Supporting comments from NPCC

Likes 0	
Dislikes 0	

Response

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	Yes
Document Name	

Comment

None

Likes 0	

Dislikes 0	
Response	
Julie Hall - Entergy - 6, Group Name Entergy	
Answer	Yes
Document Name	
Comment	
Please see comments for Question 4.	
Likes 0	
Dislikes 0	
Response	
Brandon McCormick - Brandon McCormick On Behalf of: Carol Chinn, Florida Municipal Power Agency, 6, 4, 3, 5; Chris Gowder, Florida Municipal Power Agency, 6, 4, 3, 5; David Owens, Gainesville Regional Utilities, 3, 1, 5; Ginny Beigel, City of Vero Beach, 3; Joe McKinney, Florida Municipal Power Agency, 6, 4, 3, 5; Mike Blough, Kissimmee Utility Authority, 5, 3; Richard Montgomery, Florida Municipal Power Agency, 6, 4, 3, 5; Tom Reedy, Florida Municipal Power Pool, 6; - Brandon McCormick, Group Name FMPA	
Answer	Yes
Document Name	
Comment	
No comment	
Likes 0	
Dislikes 0	
Response	
Russell Noble - Cowlitz County PUD - 3,5	
Answer	Yes
Document Name	
Comment	
Cowlitz PUD supports the comments submitted by Brian Evans-Mongeon, Utility Services Inc.	
Likes 0	

Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5	
Answer	Yes
Document Name	
Comment	
No comments.	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern does not foresee this change altering our categorization of existing BES Cyber Assets.	
Likes 0	
Dislikes 0	
Response	
Linda Jacobson-Quinn - City of Farmington - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Sandra Pacheco - Silicon Valley Power - City of Santa Clara - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Val Ridad - Silicon Valley Power - City of Santa Clara - 3,4,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeff Ipsaro - Silicon Valley Power - City of Santa Clara - 3,4,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Maier - Intermountain REA - 3	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Kristine Ward - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
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	
Aaron Austin - AEP - 3,5	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jonathan Aragon - APS - Arizona Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 1	CMS Energy - Consumers Energy Company, 4, Martinez Theresa

Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8,9 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1,3,5 - WECC	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Marty Hostler - Northern California Power Agency - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Douglas Johnson - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 3, Group Name FirstEnergy Corporation	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Larry Watt - Lakeland Electric - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Ellen Oswald - Midcontinent ISO, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Anderson - CMS Energy - Consumers Energy Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrey Komissarov - Sempra - San Diego Gas and Electric - 7 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Dennis Sismaet - Northern California Power Agency - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dmitriy Bazylyuk - NiSource - Northern Indiana Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jack Cashin - American Public Power Association - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Wendy Center - U.S. Bureau of Reclamation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion, NextEra and HQ	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF	
Answer	
Document Name	
Comment	
The NSRF cannot answer this question as we do not know the configuration within every member of NERC. Please see the second paragraph to question 1.	
Likes 1	OGE Energy - Oklahoma Gas and Electric Co., 3, Hargrove Donald
Dislikes 0	
Response	
Joel Charlebois - AESI - Acumen Engineered Solutions International Inc. - 5	
Answer	
Document Name	
Comment	
No. CIP-002-5.1a impact rating criterion 2.11. See response to question #1.	
Likes 0	
Dislikes 0	

Response
Thomas Breene - WEC Energy Group, Inc. - 3
Answer	
Document Name	
Comment
We support the MRO NSRF comments.
Likes 0	
Dislikes 0	
Response
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI
Answer	
Document Name	
Comment
AECI supports comments provided by NRECA
Likes 0	
Dislikes 0	
Response
Rachel Coyne - Texas Reliability Entity, Inc. - 10
Answer	
Document Name	
Comment
Please see Texas RE’s response to #1.
Likes 0	
Dislikes 0	
Response

4. Control Center definition: Is there a scenario where a Control Center hosts both the inclusion personnel and the exclusion personnel? If yes, please provide them here.

Heather Morgan - EDP Renewables North America LLC - 5

Answer	No
Document Name	

Comment

EDPR NA is not aware of the scenario ocnsisting of both inclusion and exclusion personnel.

Likes 0	
Dislikes 0	

Response

George Brown - Acciona Energy North America - 5

Answer	No
Document Name	

Comment

Supporting the MRO NSRF's comments.

Likes 0	
Dislikes 0	

Response

Kenya Streeter - Edison International - Southern California Edison Company - 6

Answer	No
Document Name	

Comment

Please refer to comments submitted by Robert Blackney on behalf of Southern California Edison

Likes 0	
Dislikes 0	

Response

Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	No
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 5	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	

Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Ellen Oswald - Midcontinent ISO, Inc. - 2	
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	
Chris Scanlon - Exelon - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Stephanie Burns - Stephanie Burns On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Stephanie Burns	

Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Douglas Johnson - American Transmission Company, LLC - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Marty Hostler - Northern California Power Agency - 5,6	
Answer	No
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1,3,5 - WECC	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Faz Kasraie - Seattle City Light - 5 - WECC	
Answer	No

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8,9 - WECC	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jonathan Aragon - APS - Arizona Public Service Co. - 6	
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	
Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Maier - Intermountain REA - 3	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeff Ipsaro - Silicon Valley Power - City of Santa Clara - 3,4,5	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Val Ridad - Silicon Valley Power - City of Santa Clara - 3,4,5	

Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion, NextEra and HQ	
Answer	Yes
Document Name	
Comment	
Unless modified to limit to two or more locations, the inclusion qualifier 5 could include control building within a substation. For small locations, one person may fulfill both roles (at different times)	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Please see the comments provided under question 1 for examples of possible inclusion/exclusion conflicts. Southern Company believes there are situations that exist where there is the potential to have an inclusion / exclusion conflict for business units that may partially meet an inclusion and exclusion at the same time. For example, Southern Company has a centrally located dispatch center that develops specific dispatch instructions for economics under the constraints of reliability as determined by the BA and RC, and reliability dispatch instructions from the BA and RC are relayed through the dispatch center without making modifications. The use of “develop dispatch instructions” versus using the NERC defined term “Operating Instruction” may create confusion and ambiguity regarding applicability.	

Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
One example as suggested above, without adding an exclusion for Information Technology and Operational Technology personnel allows for them to perform their tasks related to their job descriptions without limiting the number of locations that they can be connected and communicating to at any given time, or inadvertently including them as operating personnel should they occupy a desk in a Control Center or associated data center.	
Likes 0	
Dislikes 0	
Response	
Jack Cashin - American Public Power Association - 4	
Answer	Yes
Document Name	
Comment	
It may be possible for a single person to fit both operating personnel revised definition, as well as the definition of excluded personnel, but at different times. This can happen at smaller organizations where individuals perform multiple roles. It is also possible for management or engineering staff to be identified as operating personnel due to their qualifications, while not actually performing the operator function.	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	Yes

Document Name	
Comment	
One example could be GOP inclusion personnel located at a plant site where there are also excluded unit operators.	
Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Darnez Gresham On Behalf of: Annette Johnston, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Darnez Gresham	
Answer	Yes
Document Name	
Comment	
One example could be GOP inclusion personnel located at a plant site where there are also excluded unit operators.	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5	
Answer	Yes
Document Name	
Comment	
No comments.	
Likes 0	
Dislikes 0	
Response	
Dmitriy Bazylyuk - NiSource - Northern Indiana Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	

During the Loss of Primary Control Center Event (Real or Test), Dispatch Operator (TO) at Back Up Control Center (BUCC) may act as a TOP while Transmission System Supervisors (TOP) are in transit to the BUCC.

Likes 0	
Dislikes 0	

Response

Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1

Answer	Yes
Document Name	

Comment

We support the following RSC comment : Unless modified to limit to two or more locations, the inclusion qualifier 5 could include control building within a substation.

For small locations, one person may fulfill both roles (at different times)

Likes 0	
Dislikes 0	

Response

Russell Noble - Cowlitz County PUD - 3,5

Answer	Yes
Document Name	

Comment

Cowlitz PUD supports the comments submitted by Brian Evans-Mongeon, Utility Services Inc.

Likes 0	
Dislikes 0	

Response

Brandon McCormick - Brandon McCormick On Behalf of: Carol Chinn, Florida Municipal Power Agency, 6, 4, 3, 5; Chris Gowder, Florida Municipal Power Agency, 6, 4, 3, 5; David Owens, Gainesville Regional Utilities, 3, 1, 5; Ginny Beigel, City of Vero Beach, 3; Joe McKinney, Florida Municipal Power Agency, 6, 4, 3, 5; Mike Blough, Kissimmee Utility Authority, 5, 3; Richard Montgomery, Florida Municipal Power Agency, 6, 4, 3, 5; Tom Reedy, Florida Municipal Power Pool, 6; - Brandon McCormick, Group Name FMPA

Answer	Yes

Document Name	
Comment	

FMPA agrees with the following comments from APPA:

It may be possible for a single person to fit both operating personnel revised definition, as well as the definition of excluded personnel, but at different times. This can happen at smaller organizations where individuals perform multiple roles.

It is also possible for management or engineering staff to be identified as operating personnel due to their qualifications, while not actually performing the operator function.

Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	

It may be possible for a single person to fulfil both roles, maybe at different times. This may be more likely to occur in smaller organizations where individuals perform multiple roles.

Management or engineering staff may also be identified as operating personnel when qualified to, but not performing the operator function.

Likes 0	
Dislikes 0	
Response	
Julie Hall - Entergy - 6, Group Name Entergy	
Answer	Yes
Document Name	
Comment	

The operation of a Transmission Owner breaker may be shared between the Transmission Operator and Generator Operator not centrally dispatched. In such a case, the shared breaker(s) may exist on a ring bus where there is no separate breaker to isolate the generator Facility from the ring bus, or a similar scenario involving a breaker and a half scheme. The use of the undefined term “plant operator” does not exclude the Generator Operator from operating a Transmission Owner breaker. The same situation may occur with distribution customers, retail or commercial, which may have the ability to operate a Transmission Owner breaker due to not having separate isolation equipment.

NOTE: Typically a Generator Operator which has a need to operate the shared Transmission Owner breaker will submit an outage request to the Balancing Authority, Reliability Coordinator, and/or Transmission Operator. Unsure about distribution customer outages.

Likes 0	
Dislikes 0	

Response

Larry Watt - Lakeland Electric - 1

Answer	Yes
Document Name	

Comment

It may be possible for a single person to fit both operating personnel revised definition, as well as the definition of excluded personnel, but at different times. This can happen at smaller organizations where individuals perform multiple roles.

It is also possible for management or engineering staff to be identified as operating personnel due to their qualifications, while not actually performing the operator function.

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

Has the drafting team considered a scenario in which there could be two separate facilities that could both potentially fall under the proposed definition, that are housed inside the same Physical Security Perimeter (PSP)? With both facilities being inside the same PSP, would this be considered to be one Control Center or two separate Control Centers?

Likes 0	
Dislikes 0	

Response

Thomas Breene - WEC Energy Group, Inc. - 3

Answer	Yes
Document Name	

Comment	
We support the MRO NSRF comments.	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
BPA believes the current language in the exclusion section isn't clear enough to determine whether personnel can fall within both inclusion and exclusion. Based on current language, it is unclear whether personnel at a centrally located dispatch center could fall within both inclusion and exclusion.	
Likes 0	
Dislikes 0	
Response	
Peter Yost - Con Ed - Consolidated Edison Co. of New York - 3	
Answer	Yes
Document Name	
Comment	
Supporting comments from NPCC	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	Yes
Document Name	
Comment	

City Light supports SRP comments

Likes 0	
Dislikes 0	

Response

Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF

Answer	Yes
Document Name	

Comment

There may be an Entity who is vertically integrated and host those Functions in separate locations due to their apparent size.

Likes 0	
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion

Answer	Yes
Document Name	

Comment

Yes, but it appears that even if there are any inclusion personnel it doesn't matter if there are any exclusion personnel because by definition it's a Control Center.

Likes 0	
Dislikes 0	

Response

Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1

Answer	Yes
Document Name	

Comment

By Agreement with our TOP, during emergency conditions we have staff that potentially can meet the included staff for "...operat[ing] or direct[ing] the operation of a Transmission Owner's BES Transmission Facilities in Realtime." Under Normal conditions we have "...plant operators located at a

generator plant site or personnel at a centrally located dispatch center who relay dispatch instructions without making any modifications."	
Likes 0	
Dislikes 0	
Response	
Aaron Austin - AEP - 3,5	
Answer	Yes
Document Name	
Comment	
Potentially yes, but AEP is not aware of any specific instances. The words of the definition could be changed to only exclude if there are no inclusions to get ahead of any possible issues. AEP suggests the SDT change the definition as follows: “Operating personnel do not include if they are the only operating personnel located at the asset:”	
Likes 0	
Dislikes 0	
Response	
Sandra Pacheco - Silicon Valley Power - City of Santa Clara - 5	
Answer	Yes
Document Name	
Comment	
Erroneous Response: I would like to change my answer from Yes to No.	
Likes 0	
Dislikes 0	
Response	
Andrey Komissarov - Sempra - San Diego Gas and Electric - 7 - WECC	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 3, Group Name FirstEnergy Corporation	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Linda Jacobson-Quinn - City of Farmington - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Warren Cross - ACES Power Marketing - 1,3,4,5 - MRO,Texas RE,SERC,SPP RE,RF, Group Name ACES Standards Collaborators	
Answer	
Document Name	
Comment	
No comment.	
Likes 0	
Dislikes 0	
Response	

Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Please see Texas RE's response to #1.	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	
Document Name	
Comment	
AECI supports comments provided by NRECA	
Likes 0	
Dislikes 0	
Response	
Joel Charlebois - AESI - Acumen Engineered Solutions International Inc. - 5	
Answer	
Document Name	
Comment	
Yes. For GOP Control Centers, there may be operating personnel who can develop specific dispatch instructions for generation Facilities at two or more locations as part of their job function, and other operating personnel who simply operate (start/stop/etc) or relay the developed dispatch instructions.	
Likes 0	
Dislikes 0	
Response	

5. Implementation Plan: The new Control Center definition will become effective on the first day of the first calendar quarter that is three (3) calendar months after the effective date of the applicable governmental authority's order approving the term, or as otherwise provided for by the applicable governmental authority. Do you agree that three calendar months is enough time to update documentation? If you do not agree, please provide the amount of time needed and types of actions that will need to be completed during this time.

Leonard Kula - Independent Electricity System Operator - 2

Answer	No
Document Name	

Comment

The IESO submits that the implimentation plan should allow an RE to update its documentation during its regular review cycle. This will help avoid duplication of effort. It should also consider any potentially significant changes required for Control Center physical and logical changes to occur within budget cycles.

Likes 0	
Dislikes 0	

Response

Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1

Answer	No
Document Name	

Comment

In some cases there may be a need to implement security measures not considered prior to the reclassification. Depending on the budget period and cycle, these would be unbudgeted and may take up to a year to complete.

Likes 0	
Dislikes 0	

Response

Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF

Answer	No
Document Name	

Comment

For those entities that may need to start some programs from scratch, they will need more time. Recommend that the Implementation time line be pushed to 12 months.

Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,4,5 - RF	
Answer	No
Document Name	
Comment	
If the definition is a defined term being used by multiple reliability standards, 18 calendar months will be more appropriate to implement the revised definition.	
Likes 1	CMS Energy - Consumers Energy Company, 4, Martinez Theresa
Dislikes 0	
Response	
ALAN ADAMSON - New York State Reliability Council - 10	
Answer	No
Document Name	
Comment	
The Implementation Plan does not allow enough time to bring newly-identified Control Centers into compliance.	
Likes 0	
Dislikes 0	
Response	
Peter Yost - Con Ed - Consolidated Edison Co. of New York - 3	
Answer	No
Document Name	
Comment	
Supporting comments from NPCC.	
Likes 0	
Dislikes 0	

Response
Thomas Breene - WEC Energy Group, Inc. - 3
Answer	No
Document Name	
Comment
We do not believe the definition can be implemented as proposed and hesitate to suggest an alternative timeframe until we see a revised definition however 12 months may be more appropriate than 3 months.
Likes 0	
Dislikes 0	
Response
Kenya Streeter - Edison International - Southern California Edison Company - 6
Answer	No
Document Name	
Comment
Please refer to comments submitted by Robert Blackney on behalf of Southern California Edison
Likes 0	
Dislikes 0	
Response
sean erickson - Western Area Power Administration - 1
Answer	No
Document Name	
Comment
WAPA agrees with the NSRF comment that for those entities that may need to start some programs from scratch, they will need more time. Recommend that the Implementation time line be pushed to 12 months.
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	
Duke Energy disagrees with the proposed Implementation Plan of three (3) calendar months. The change to the definition of Control Center would necessitate a review of all internal procedures in which it is referenced to determine if said procedure would need to be updated. The review and analysis, coupled with the training that would be necessary if changes to a procedure were implemented would take much longer than three months. Duke Energy recommends an Implementation Plan of twelve (12) months. This would give industry enough time to do internal reviews, make changes where necessary, and train on said changes prior to the new definition going into effect.	
Likes 0	
Dislikes 0	
Response	
Stephanie Burns - Stephanie Burns On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Stephanie Burns	
Answer	No
Document Name	
Comment	
See EEI Comments.	
Likes 0	
Dislikes 0	
Response	
Larry Watt - Lakeland Electric - 1	
Answer	No
Document Name	
Comment	
Three months should be acceptable if implementation of the revised definition does not result in the identification of a new Control Center. It should be made clear that identification of a new Control Center would be an “unplanned change” and therefore provide an additional one or two years to meet the requirements.	
Likes 0	

Dislikes 0	
Response	
Julie Hall - Entergy - 6, Group Name Entergy	
Answer	No
Document Name	
Comment	
The three (3) calendar months would not allow enough time to make the needed procedure updates. Recommend six (6) calendar months.	
Likes 0	
Dislikes 0	
Response	
Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	No
Document Name	
Comment	
While the Implementation Plan for CIP standard compliance, coupled with the proposed Planned and Unplanned Changes language in the proposed CIP-002-6, is adequate, the Implementation Plan needs to be changed for non-CIP standard compliance. NRECA strongly recommends that language and timeframes similar to the Planned and Unplanned Changes language should be added to the Implementation Plan for non-CIP standards compliance. Without this change, registered entities will only have a little more than three months to be in compliance with non-CIP standards that include the defined term Control Center in the standard/requirement language.	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	
If the changes needed to demonstrate compliance with this change amounts to more than a simple document change then there needs to be additional time to accommodate the changes. We would suggest 12 months for implementation.	

Likes 0	
Dislikes 0	

Response

James Anderson - CMS Energy - Consumers Energy Company - 1

Answer	No
Document Name	

Comment

If the definition is a defined term being used by multiple reliability standards, 18 calendar months will be more appropriate to implement the revised definition.

Likes 0	
Dislikes 0	

Response

Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1

Answer	No
Document Name	

Comment

We support the following RSC comment : It should be made clear that this new identification would be an “unplanned change” and allow for the additional one or two years for implementation as proposed in the CIP-002 revisions.

The Implementation Plan should state that any facilities that are newly identified as Control Centers as a result of the revised definition will have 24 months to meet newly applicable compliance requirements that apply to those Control Centers.The Implementation plan should allow an RE to update its documentation during its regular review cycle. This will help avoid duplication of effort. It should also consider any potentially significant changes required for Control Center physical and logical changes to occur within budget cycles.

Likes 0	
Dislikes 0	

Response

Dmitriy Bazylyuk - NiSource - Northern Indiana Public Service Co. - 5

Answer	No
Document Name	

Comment

The changes would likely take more time than 3 months to implement. 12 calendar months would be reasonable to make sure the processes and documentation are ready.

Likes 0	
Dislikes 0	

Response

George Brown - Acciona Energy North America - 5

Answer	No
Document Name	

Comment

Supporting the MRO NSRF's comments.

Likes 0	
Dislikes 0	

Response

Heather Morgan - EDP Renewables North America LLC - 5

Answer	No
Document Name	

Comment

Due to the proposed definition of “Control Center” and its impact to numerous NERC Standards, longer time should be given to allow Registered Entities appropriate time to reevaluate CIP-002 as well as several other NERC Standards.

Likes 0	
Dislikes 0	

Response

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5

Answer	No
Document Name	

Comment
The questions relies on the revision of the definition only required administrative work associated with documentation. There is a concern that the revised definition will place equipment and/or facilities within scope of Standards that were previously not addressing the equipment and/or facility.

Likes 0	
Dislikes 0	

Response

Darnez Gresham - Darnez Gresham On Behalf of: Annette Johnston, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Darnez Gresham	
Answer	No
Document Name	

Comment
Until the scope of the revised definition is concrete, there isn’t certainty in how long it could take to implement changes, if there are any.

Likes 0	
Dislikes 0	

Response

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	

Comment
Until the scope of the revised definition is concrete, there isn’t certainty in how long it could take to implement changes, if there are any.

Likes 0	
Dislikes 0	

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	

Comment
Until the scope of the revised definition is concrete, there isn't certainty in how long it could take to implement changes, if there are any.

Likes 0	
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No
Document Name	

Comment
Southern Company feels that 12 months is a more reasonable timeframe for implementation *if* Order 693 facilities are impacted by this change or if an entity is required to start a program from the ground up.

Likes 0	
Dislikes 0	

Response

Wendy Center - U.S. Bureau of Reclamation - 5	
Answer	No
Document Name	

Comment
Reclamation recommends the new Control Center definition become effective on the first day of the first calendar quarter that is eighteen (18) calendar months after the effective date of the applicable governmental authority's order approving the definition to allow entities time to evaluate the impact of the changes effected by the new definition and implement an appropriate response. This will allow registered entities time to evaluate the impact of the new definition on their facilities and determine any necessary changes.

Likes 0	
Dislikes 0	

Response

Warren Cross - ACES Power Marketing - 1,3,4,5 - MRO,Texas RE,SERC,SPP RE,RF, Group Name ACES Standards Collaborators	
Answer	No
Document Name	
Comment	
For those entities now considered a Control Center and not a Control Room, we recommend that the Implementation time line be 18 months.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion, NextEra and HQ	
Answer	No
Document Name	
Comment	
It should be made clear that this new identification would be an “unplanned change” and allow for the additional one or two years for implementation as proposed in the CIP-002 revisions. The Implementation Plan should state that any facilities that are newly identified as Control Centers as a result of the revised definition will have 24 months to meet newly applicable compliance requirements that apply to those Control Centers. The Implementation plan should allow an RE to update its documentation during its regular review cycle. This will help avoid duplication of effort. It should also consider any potentially significant changes required for Control Center physical and logical changes to occur within budget cycles.	
Likes 0	
Dislikes 0	
Response	
David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	No
Document Name	
Comment	

If the new definition will bring new Control Centers into the scope of CIP Compliance then the three calendar months are not enough to complete all the activities required for compliance.

Likes 0	
Dislikes 0	

Response

Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 3

Answer	No
Document Name	

Comment

PNM agrees with EEI's 12 month proposal/comments.

Likes 0	
Dislikes 0	

Response

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group

Answer	No
Document Name	

Comment

The SPP Standards Review Group feels that this isn't enough time to get everything implemented. We suggest one year (1) in the event that an entity needs to get an unidentified Control Center into compliance.

Likes 0	
Dislikes 0	

Response

Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2

Answer	No
Document Name	

Comment

Based on significance of possibly changing the impact rating of a BES asset, this should take place on an implementation timeline that allows sufficient time for entities to verify their compliance with the operations and planning standards noted. The implementation and enforcement timelines for CIP-002 have been addressed, but the timeline for the other non-CIP standards has not been addressed.	
Likes 0	
Dislikes 0	
Response	
Faz Kasraie - Seattle City Light - 5 - WECC	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Aaron Austin - AEP - 3,5	
Answer	Yes
Document Name	
Comment	
Knowing that the FERC will determine the effective dates, AEP believes the Implementation Plans for the revised Control Center definition and proposed CIP-002-6 should be synchronized so the transition is less impactful.	
Likes 0	
Dislikes 0	

Response	
Jonathan Aragon - APS - Arizona Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
AZPS agrees with the exception to the initial implementation of CIP-002-6 as set forth in “Implementation Plan”.	
Likes 0	
Dislikes 0	

Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	Yes
Document Name	
Comment	
City Light supports SRP comments	
Likes 0	
Dislikes 0	

Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Yes, if the language is adjusted in 5. to add “at two or more locations.”	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Three months would be acceptable if the definition does not result in the new identification of a Control Center. It should be made clear that this new identification would be an “unplanned change” and allow for the additional one or two years for implementation.	
Likes 0	
Dislikes 0	
Response	

Brandon McCormick - Brandon McCormick On Behalf of: Carol Chinn, Florida Municipal Power Agency, 6, 4, 3, 5; Chris Gowder, Florida Municipal Power Agency, 6, 4, 3, 5; David Owens, Gainesville Regional Utilities, 3, 1, 5; Ginny Beigel, City of Vero Beach, 3; Joe McKinney, Florida Municipal Power Agency, 6, 4, 3, 5; Mike Blough, Kissimmee Utility Authority, 5, 3; Richard Montgomery, Florida Municipal Power Agency, 6, 4, 3, 5; Tom Reedy, Florida Municipal Power Pool, 6; - Brandon McCormick, Group Name FMPA	
Answer	Yes
Document Name	
Comment	
FMPA agrees with the following comments from APPA: Three months should be acceptable if implementation of the revised definition does not result in the identification of a new Control Center. It should be made clear that identification of a new Control Center would be an “unplanned change” and therefore provide an additional one or two years to meet the requirements	
Likes 0	
Dislikes 0	
Response	
Russell Noble - Cowlitz County PUD - 3,5	
Answer	Yes
Document Name	
Comment	
Cowlitz PUD supports the comments submitted by Brian Evans-Mongeon, Utility Services Inc.	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5	
Answer	Yes
Document Name	
Comment	
No comments.	
Likes 0	
Dislikes 0	

Response	
Jack Cashin - American Public Power Association - 4	
Answer	Yes
Document Name	
Comment	
Three months should be acceptable if implementation of the revised definition does not result in the identification of a new Control Center. It should be made clear that identification of a new Control Center would be an “unplanned change” and therefore provide an additional one or two years to meet the requirements.	
Likes 0	
Dislikes 0	
Response	
Linda Jacobson-Quinn - City of Farmington - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sandra Pacheco - Silicon Valley Power - City of Santa Clara - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Val Ridad - Silicon Valley Power - City of Santa Clara - 3,4,5	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeff Ipsaro - Silicon Valley Power - City of Santa Clara - 3,4,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Maier - Intermountain REA - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kristine Ward - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8,9 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1,3,5 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Marty Hostler - Northern California Power Agency - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Douglas Johnson - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 3, Group Name FirstEnergy Corporation	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ellen Oswald - Midcontinent ISO, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrey Komissarov - Sempra - San Diego Gas and Electric - 7 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Dennis Sismaet - Northern California Power Agency - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joel Charlebois - AESI - Acumen Engineered Solutions International Inc. - 5	
Answer	

Document Name	
Comment	
Yes we agree, assuming there are appropriate implementation plans in place for all affected standards and requirements that allow newly identified Control Centers brought into scope by the proposed definition sufficient time to come into compliance with such standards and requirements. If such implementation plans for all affected standards and requirements do not currently exist or do not currently address newly identified Control Centers, then we suggest that the SDT review all affected standards and requirements to develop an appropriate implementation plan for each of those, or otherwise lengthen the effective date of the proposed definition to an appropriate duration to allow newly identified Control Centers sufficient time to come into compliance with all applicable standards and requirements.	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	
Document Name	
Comment	
AECI supports comments provided by NRECA	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE does not have comments on this question.	
Likes 0	
Dislikes 0	
Response	

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Control Center Definition

Consideration of Comments | May 2018

Background

The Project 2016-02 Modifications to Critical Infrastructure Protection (CIP) Standard Drafting Team (SDT) thanks all commenters who submitted comments on the draft Control Center definition. This definition was posted for a 45-day public comment period through Friday, April 30, 2018. Stakeholders were asked to provide feedback on the definition and implementation document through a special electronic comment form. There were 74 sets of responses, including comments from approximately 177 different people from approximately 127 companies representing the 10 Industry Segments as shown in the table on the following pages.

All comments submitted can be reviewed in their original format on the project page.

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process. If you feel there has been an error or omission, you can contact the Standards Developer Jordan Mallory (via email) or at (404) 446-2589.

Control Center Definition

The CIP Modifications SDT has been responding to a Federal Energy Regulatory Commission (FERC) directive in Order No. 822 concerning protecting the communications between Control Centers, culminating in a proposed CIP-012 standard. During our discussions, we discovered that CIP-012 highlighted some issues primarily with certain substation or generating plant locations that may also relate to the current definition of Control Center.

An example of one issue is field assets such as substation control houses or plant control rooms that may host operating personnel and have communications from their remote terminal units (RTUs) to a Control Center. If these locations currently have or add a remote human-machine interface, or have some other way to affect a unit or breaker at another “geographic location,” then the location could possibly be classified as both a generating resource or substation and a Control Center. In that case, the RTU communication would fall within the scope of CIP-012. The scope of CIP-012 is not intended to include this communication, and implementing the required protection may not be feasible.

The SDT proposed a revised Control Center definition to resolve the issue of Control Center misclassification and adopted language from PER-005-2 to clarify the term “operating personnel” by excluding plant operators and substation field switching personnel with the goal of preventing field assets from being identified as Control Centers when a location does not meet the SDTs understanding of the intent of the Control Center definition. However, based on industry feedback, there are several unintended consequences to this approach. The SDT has decided to address this specific issue by excluding Control Centers that only communicate Real-time Assessment and Real-time monitoring data about the single facility where the Control Center is located from CIP-012.

Other issues were pointed out by entities concerning elements of the currently approved definition, including ambiguity around terms such as “hosting”, “operating personnel”, and “associated data centers” and concerns around authority to operate versus a system’s capability to operate. The core issue is that this facility-based Control Center definition is being used to handle different scenarios for different purposes. One concerns many other non-CIP NERC standards that apply to traditional Control Centers for Balancing Authorities, Reliability Coordinators, and Transmission Operators that have been certified by the Electric Reliability Organization Enterprise and are under the direction of NERC certified System Operators. The intent of the CIP Reliability Standards is for control systems to be identified and categorized based more on their span of control rather than the building or room they are located in or the role of the person using them. However, our inherited constructs that date back to 2003 in the CIP standards have us looking for these systems in Control Centers. This is causing the definition of Control Center to be stretched from a CIP perspective to entities that are not Control Centers from other perspectives so that we can ensure the protection of these control systems. The SDT recognizes that these matters are outside of our Standards Authorization Request (SAR).

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Nomination Form

Project Number 2016-02 Modifications to CIP Standards

Do not use this form for submitting nominations. Use the electronic form to submit nominations by **8 p.m. Eastern, Wednesday, May 23, 2018.** This unofficial version is provided to assist nominees in compiling the information necessary to submit the electronic form.

Additional information can be found on the Project 2016-02 Modifications to the CIP Standards page. If you have questions, contact Standards Developer, Jordan Mallory (via email), or at 404-446-2589.

By submitting a nomination form, you are indicating your willingness and agreement to actively participate in face-to-face meetings and conference calls.

Previous drafting or review team experience is beneficial, but not required. A brief description of the desired qualifications, expected commitment, and other pertinent information is included below.

Project 2016-02 Modifications to CIP Standards

This solicitation for nominations is to augment the existing Project 2016-02 Modifications to CIP Standards drafting team that is continuing to address the Standards Authorization Request. NERC is seeking individuals from the United States and Canada who possess experience in one or more of the following areas, but are not limited to:

- Virtualization;
- Cyber Asset and BES Cyber Asset Definitions; and
- Network and Externally Accessible Devices.

Standards Affected

CIP-002-5.1, CIP-003-6, CIP-004-6, CIP-005-5, CIP-006-6, CIP-007-6, CIP-008-5, CIP-009-6, CIP-010-2, CIP-011-2, and CIP-012-1.

The time commitment for this project is expected to be up to two face-to-face meetings per quarter (on average two full working days each meeting) with conference calls scheduled as needed to meet the agreed-upon timeline the review or drafting team sets forth. Team members may also have side projects, either individually or by subgroup, to present to the larger team for discussion and review. Lastly, an important component of the review and drafting team effort is outreach. Members of the team will be expected to conduct industry outreach during the development process to support a successful project outcome.

Name:	
Organization:	
Address:	
Telephone:	
E-mail:	

Please briefly describe your experience and qualifications to serve on the requested Standard Drafting Team (Bio):

If you are currently a member of any NERC drafting team(s), please list each one here:

☐ Not currently on any active SAR or standard drafting team.

☐ Currently a member of the following SAR or standard drafting team(s):

If you previously worked on any NERC drafting team(s), please identify each one here:

☐ No prior NERC SAR or standard drafting team.

☐ Prior experience on the following team(s):

Select each NERC Region in which you have experience relevant to the Project for which you are volunteering:

☐ Texas RE	☐ NPCC	☐ SPP RE
☐ FRCC	☐ RF	☐ WECC
☐ MRO	☐ SERC	☐ NA – Not Applicable

Select each Industry Segment that you represent:	
☐	1 — Transmission Owners
☐	2 — RTOs, ISOs
☐	3 — Load-serving Entities
☐	4 — Transmission-dependent Utilities
☐	5 — Electric Generators
☐	6 — Electricity Brokers, Aggregators, and Marketers
☐	7 — Large Electricity End Users
☐	8 — Small Electricity End Users
☐	9 — Federal, State, and Provincial Regulatory or other Government Entities
☐	10 — Regional Reliability Organizations and Regional Entities
☐	NA – Not Applicable

Select each Function[1] in which you have current or prior expertise:	
☐ Balancing Authority	☐ Transmission Operator
☐ Compliance Enforcement Authority	☐ Transmission Owner
☐ Distribution Provider	☐ Transmission Planner
☐ Generator Operator	☐ Transmission Service Provider
☐ Generator Owner	☐ Purchasing-selling Entity
☐ Interchange Authority	☐ Reliability Coordinator
☐ Load-serving Entity	☐ Reliability Assurer
☐ Market Operator	☐ Resource Planner
☐ Planning Coordinator	

[1] These functions are defined in the NERC Functional Model, which is available on the NERC web site.

Provide the names and contact information of two references who could attest to your technical qualifications and your ability to work well in a group:			
Name:		Telephone:	
Organization:		E-mail:	
Name:		Telephone:	
Organization:		E-mail:	
Provide the name and contact information of your immediate supervisor or a member of your management who can confirm your organization's willingness to support your active participation.			
Name:		Telephone:	
Title:		Email:	

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2016-02 Modifications to CIP Standards

Nomination Period Open through May 23, 2018

Now Available

Nominations are being sought for additional standard drafting team members through **8 p.m. Eastern, Wednesday, May 23, 2018**.

Use the electronic form to submit a nomination. If you experience difficulties using the electronic form, contact Wendy Muller. An unofficial Word version of the nomination form is posted on the Standard Drafting Team Vacancies and the project page.

By submitting a nomination form, you are indicating your willingness and agreement to actively participate in face-to-face meetings and conference calls.

The time commitment for this project is expected to be up to two face-to-face meetings per quarter (on average two full working days each meeting) with conference calls scheduled as needed to meet the agreed-upon timeline the review or drafting team sets forth. Team members may also have side projects, either individually or by subgroup, to present to the larger team for discussion and review. Lastly, an important component of the review and drafting team effort is outreach. Members of the team will be expected to conduct industry outreach during the development process to support a successful project outcome.

Previous drafting or review team experience is beneficial, but not required.

Project 2016-02 Modifications to CIP Standards

This solicitation for nominations is to augment the existing Project 2016-02 Modifications to CIP Standards drafting team that is continuing to address the Standards Authorization Request. NERC is seeking individuals from the United States and Canada who possess experience in one or more of the following areas, but are not limited to:

- Virtualization;
- Cyber Asset and BES Cyber Asset Definitions; and
- Network and Externally Accessible Devices.

Standards Affected

CIP-002-5.1, CIP-003-6, CIP-004-6, CIP-005-5, CIP-006-6, CIP-007-6, CIP-008-5, CIP-009-6, CIP-010-2, CIP-011-2, and CIP-012-1.

Next Steps

The Standards Committee is expected to appoint members to the team in June 2018. Nominees will be notified shortly after they have been appointed.

For information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact Mat Bunch at (404) 446-9785 or Jordan Mallory at (404) 446-2589.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the fourth draft of the proposed standard.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23 - April 21, 2016
SAR posted for comment	June 1 – June 30, 2016
Informal comment period	February 10- March 13, 2017
45-day formal comment period with initial ballot	July 27 – September 11, 2017
45-day formal comment period with additional ballot	October 27 – December 11, 2017
45-day formal comment period with additional ballot	March 16 – April 30, 2018
45-day formal comment period with additional ballot	May 18 – July 2, 2018

Anticipated Actions	Date
10-day final ballot	July 30 – August 8, 2018
NERC Board	August 16, 2018

A. Introduction

1. **Title:** Cyber Security – Communications between Control Centers

2. **Number:** CIP-012-1

3. **Purpose:** To protect the confidentiality and integrity of Real-time Assessment and Real-time monitoring data transmitted between Control Centers.

4. **Applicability:**

   4.1. Functional Entities: The requirements in this standard apply to the following functional entities, referred to as "Responsible Entities," that own or operate a Control Center.

   4.1.1. Balancing Authority

   4.1.2. Generator Operator

   4.1.3. Generator Owner

   4.1.4. Reliability Coordinator

   4.1.5. Transmission Operator

   4.1.6. Transmission Owner

   4.2. Exemptions: The following are exempt from Reliability Standard CIP-012-1:

   4.2.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

   4.2.2. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

   4.2.3. A Control Center at a generation resource or Transmission station or substation that transmits to another Control Center Real-time Assessment or Real-time monitoring data pertaining only to the generation resource or Transmission station or substation at which the transmitting Control Center is located.

5. **Effective Date:** See Implementation Plan for CIP-012-1.

B. Requirements and Measures

R1. The Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring data while being transmitted between any applicable Control Centers. The Responsible Entity is not required to include oral communications in its plan. The plan shall include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. Identification of security protection used to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers;

1.2. Identification of where the Responsible Entity applied security protection for transmitting Real-time Assessment and Real-time monitoring data between Control Centers; and

1.3. If the Control Centers are owned or operated by different Responsible Entities, identify the responsibilities of each Responsible Entity for applying security protection to the transmission of Real-time Assessment and Real-time monitoring data between those Control Centers.

M1. Evidence may include, but is not limited to, documented plan(s) that meet the security objective of Requirement R1 and documentation demonstrating the implementation of the plan(s).

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" (CEA) means NERC, the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- The Responsible Entities shall keep data or evidence of each Requirement in this Reliability Standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	N/A	The Responsible Entity documented its plan(s) but failed to include one of the applicable Parts of the plan as specified in Requirement R1.	The Responsible Entity documented its plan(s) but failed to include two of the applicable Parts of the plan as specified in Requirement R1.	The Responsible Entity failed to document plan(s) for Requirement R1; Or The Responsible Entity failed to implement any Part of its plan(s) for Requirement R1, except under CIP Exceptional Circumstances.

D. Regional Variances

None.

E. Associated Documents

Implementation Plan.

Technical Rationale for CIP-012-1.

Implementation Guidance.

Version History

Version	Date	Action	Change Tracking
1	TBD	Respond to FERC Order No. 822	N/A

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the ~~third~~ fourth draft of the proposed standard.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23 - April 21, 2016
SAR posted for comment	June 1 – June 30, 2016
Informal comment period	February 10- March 13, 2017
45-day formal comment period with initial ballot	July 27 – September 11, 2017
45-day formal comment period with additional ballot	October 27 – December 11, 2017
45-day formal comment period with additional ballot	March 16 – April 30, 2018
45-day formal comment period with additional ballot	May 18 – July 2, 2018

Anticipated Actions	Date
~~45-day formal comment period with additional ballot~~	~~May 18 – July 2, 2018~~
10-day final ballot	July 30 – August 8, 2018
NERC Board	August 16, 2018

A. Introduction

1. **Title:** Cyber Security – Communications between Control Centers

2. **Number:** CIP-012-1

3. **Purpose:** To protect the confidentiality and integrity of Real-time Assessment and Real-time monitoring data transmitted between Control Centers.

4. **Applicability:**

   4.1. Functional Entities: The requirements in this standard apply to the following functional entities, referred to as "Responsible Entities," that own or operate a Control Center.

   4.1.1. Balancing Authority

   4.1.2. Generator Operator

   4.1.3. Generator Owner

   4.1.4. Reliability Coordinator

   4.1.5. Transmission Operator

   4.1.6. Transmission Owner

   4.2. Exemptions: The following are exempt from Reliability Standard CIP-012-1:

   4.2.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

   4.2.2. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

   4.2.3. A Control Center at a generation resource or Transmission station or substation that transmits to another Control Center Real-time Assessment or Real-time monitoring data pertaining only to the generation resource or Transmission station or substation at which the transmitting Control Center is located.

5. **Effective Date:** See Implementation Plan for CIP-012-1.

B. Requirements and Measures

R1. The Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring data while being transmitted between any applicable Control Centers. The~~is~~ Responsible Entity is not required to include ~~requirement excludes~~ oral communications in its plan. The plan shall include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. Identification of security protection used to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers;

1.2. Identification of where the Responsible Entity applied security protection ~~-~~for transmitting Real-time Assessment and Real-time monitoring data between Control Centers; and

1.3. If the Control Centers are owned or operated by different Responsible Entities, identify the responsibilities of each Responsible Entity for applying security protection to the transmission of Real-time Assessment and Real-time monitoring data between those Control Centers.

M1. Evidence may include, but is not limited to, documented plan(s) that meet the security objective of Requirement R1 and documentation demonstrating the implementation of the plan(s).

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" (CEA) means NERC, the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the ~~Compliance Enforcement Authority~~CEA may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its ~~Compliance Enforcement Authority~~CEA to retain specific evidence for a longer period of time as part of an investigation.

- The Responsible Entities shall keep data or evidence of each Requirement in this Reliability Standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The ~~Compliance Enforcement Authority~~CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	N/A	The Responsible Entity documented its plan(s) but failed to include one of the applicable Pparts of the plan as specified in Requirement R1.	The Responsible Entity documented its plan(s) but failed to include two of the applicable Pparts of the plan as specified in Requirement R1.	The Responsible Entity failed to document plan(s) for Requirement R1; Or The Responsible Entity failed to implement any Part of its plan(s) for Requirement R1, except under CIP Exceptional Circumstances.

D. Regional Variances

None.

E. Associated Documents

Implementation Plan.

Technical Rationale for CIP-012-1.

Implementation Guidance.

Version History

Version	Date	Action	Change Tracking
1	TBD	Respond to FERC Order No. 822	N/A

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2016-02 Modifications to CIP Standards
Reliability Standard CIP-012-1

Applicable Standard

- Reliability Standard CIP-012-1 - Cyber Security – Communications between Control Centers

Requested Retirements

- None

Prerequisite Standard

These standard(s) or definitions must be approved before the Applicable Standard becomes effective:

- None

Applicable Entities

- Balancing Authority
- Generator Operator
- Generator Owner
- Reliability Coordinator
- Transmission Operator
- Transmission Owner

Effective Date

Reliability Standard CIP-012-1 - Cyber Security – Communications between Control Centers

Where approval by an applicable governmental authority is required, Reliability Standard CIP-012-1 shall become effective on the first day of the first calendar quarter that is twenty-four (24) calendar months after the effective date of the applicable governmental authority's order approving the standard, or as otherwise provided for by the applicable governmental authority.

Where approval by an applicable governmental authority is not required, Reliability Standard CIP-012-1 shall become effective on the first day of the first calendar quarter that is twenty-four (24) calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Comment Form

Project 2016-02 Modifications to CIP Standards
CIP-012-1

Do not use this form for submitting comments. Use the Standards Balloting and Commenting System to submit comments on **CIP-012-1 – Cyber Security – Communications between Control Centers.** Comments must be submitted by **8 p.m. Eastern, Monday, July 2, 2018.**

Additional information is available on the project page. If you have questions, contact Jordan Mallory at (404) 446-2589.

Background

On January 21, 2016, the Commission issued Order No. 822, approving seven CIP Reliability Standards and new or modified definitions, and directing modifications to the CIP Reliability Standards. Among others, the Commission directed NERC to "develop modifications to the CIP Reliability Standards to require responsible entities to implement controls to protect, at a minimum, communication links and sensitive bulk electric system data communicated between bulk electric system Control Centers in a manner that is appropriately tailored to address the risks posed to the bulk electric system by the assets being protected (i.e., high, medium, or low impact)." (Order 822, Paragraph 53)

The Project 2016-02 Standard Drafting Team (SDT) drafted Reliability Standard CIP-012-1 to require Responsible Entities to implement controls to protect sensitive Bulk Electric System (BES) data while being transmitted over communications links between BES Control Centers. Due to the sensitivity of the data being communicated between the Control Centers, the standard applies to all impact levels (i.e., high, medium, or low impact).

The SDT drafted CIP-012-1 allowing Responsible Entities to apply protection to the links, the data, or both, in order to satisfy the security objective consistent with the capabilities of the Responsible Entity's operational environment. Requirement R1 requires Responsible Entities to implement, except under CIP Exceptional Circumstances, one or more documented plans that protect Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers. The plan(s) must address how the Responsible Entity will mitigate the risk of unauthorized disclosure or modification of the applicable data.

Questions

1. Control Center Exemption Language: The SDT drafted Exemption language in the Applicability section specifically for CIP-012-1 to exempt Control Centers that only transmit data pertaining to a single co-located substation or generating plant. Do you agree with this revision? If not, please provide the basis for your disagreement and an alternate proposal.

   ☐ Yes
   ☐ No

   Comments:

2. Requirement R1: The SDT modified Requirement R1 to state: "The Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring data while being transmitted between any applicable Control Centers. The Responsible Entity is not required to include oral communications in its plan." Do you agree with this revision? If not, please provide the basis for your disagreement and an alternate proposal.

   ☐ Yes
   ☐ No

   Comments:

3. Implementation Plan: The SDT established the Implementation Plan to make the standard effective the first day of the first calendar quarter that is twenty-four (24) calendar months after the effective date of the applicable governmental authority's order approving the standard, or as otherwise provided for by the applicable governmental authority. Do you agree with this proposal? If you think an alternate implementation time period is needed, please provide a detailed explanation of actions and time needed to meet the implementation deadline.

   ☐ Yes
   ☐ No

   Comments:

4. Technical Rationale: The SDT modified the draft Technical Rationale for CIP-012 to further explain the need for the exemption for certain Control Centers. Do you agree with the explanations and included diagrams in the draft Technical Rationale? If you do not agree, or if you agree but have comments or suggestions for the draft Technical Rationale, please provide your recommendation and explanation.

   ☐ Yes
   ☐ No

   Comments:

5. The SDT modified the draft Implementation Guidance for CIP-012 to provide examples of how a Responsible Entity could comply with the requirements. The draft Implementation Guidance does not prescribe the only approaches to compliance. Rather, it describes what the SDT believes would be effective ways to comply with the standard. See NERC's Compliance Guidance policy for information on Implementation Guidance. Do you agree with the draft Implementation Guidance? If you do not agree, or if you agree but have comments or suggestions for the draft Implementation Guidance, please provide your recommendation and explanation.

   ☐ Yes
   ☐ No

   Comments:

6. The SDT believes proposed CIP-012-1 provides entities with flexibility to meet the reliability objectives in a cost effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost effective approaches, please provide your recommendation and, if appropriate, technical justification.

   ☐ Yes
   ☐ No

   Comments:

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Violation Risk Factor and Violation Severity Level Justifications

Project 2016-02 Modifications to CIP Standards

This document provides the standard drafting team's (SDT's) justification for assignment of violation risk factors (VRFs) and violation severity levels (VSLs) for each requirement in **CIP-012-1**. Each requirement is assigned a VRF and a VSL. These elements support the determination of an initial value range for the Base Penalty Amount regarding violations of requirements in FERC-approved Reliability Standards, as defined in the Electric Reliability Organizations (ERO) Sanction Guidelines. The SDT applied the following NERC criteria and FERC Guidelines when developing the VRFs and VSLs for the requirements.

NERC Criteria for Violation Risk Factors

High Risk Requirement

A requirement that, if violated, could directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures, or could hinder restoration to a normal condition.

Medium Risk Requirement

A requirement that, if violated, could directly affect the electrical state or the capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System. However, violation of a medium risk requirement is unlikely to lead to Bulk Electric System instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System. However, violation of a medium risk requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to Bulk Electric System instability, separation, or cascading failures, nor to hinder restoration to a normal condition.

Lower Risk Requirement
A requirement that is administrative in nature and a requirement that, if violated, would not be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System; or, a requirement that is administrative in nature and a requirement in a planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.

FERC Guidelines for Violation Risk Factors

Guideline (1) – Consistency with the Conclusions of the Final Blackout Report

FERC seeks to ensure that VRFs assigned to Requirements of Reliability Standards in these identified areas appropriately reflect their historical critical impact on the reliability of the Bulk-Power System. In the VSL Order, FERC listed critical areas (from the Final Blackout Report) where violations could severely affect the reliability of the Bulk-Power System:

- Emergency operations
- Vegetation management
- Operator personnel training
- Protection systems and their coordination
- Operating tools and backup facilities
- Reactive power and voltage control
- System modeling and data exchange
- Communication protocol and facilities
- Requirements to determine equipment ratings
- Synchronized data recorders
- Clearer criteria for operationally critical facilities
- Appropriate use of transmission loading relief.

Guideline (2) – Consistency within a Reliability Standard

FERC expects a rational connection between the sub-Requirement VRF assignments and the main Requirement VRF assignment.

Guideline (3) – Consistency among Reliability Standards

FERC expects the assignment of VRFs corresponding to Requirements that address similar reliability goals in different Reliability Standards would be treated comparably.

Guideline (4) – Consistency with NERC's Definition of the Violation Risk Factor Level

Guideline (4) was developed to evaluate whether the assignment of a particular VRF level conforms to NERC's definition of that risk level.

Guideline (5) – Treatment of Requirements that Co-mingle More Than One Obligation

Where a single Requirement co-mingles a higher risk reliability objective and a lesser risk reliability objective, the VRF assignment for such Requirements must not be watered down to reflect the lower risk level associated with the less important objective of the Reliability Standard.

NERC Criteria for Violation Severity Levels

VSLs define the degree to which compliance with a requirement was not achieved. Each requirement must have at least one VSL. While it is preferable to have four VSLs for each requirement, some requirements do not have multiple "degrees" of noncompliant performance and may have only one, two, or three VSLs.

VSLs should be based on NERC's overarching criteria shown in the table below:

Lower VSL	Moderate VSL	High VSL	Severe VSL
The performance or product measured almost meets the full intent of the requirement.	The performance or product measured meets the majority of the intent of the requirement.	The performance or product measured does not meet the majority of the intent of the requirement, but does meet some of the intent.	The performance or product measured does not substantively meet the intent of the requirement.

FERC Order of Violation Severity Levels

The FERC VSL guidelines are presented below, followed by an analysis of whether the VSLs proposed for each requirement in the standard meet the FERC Guidelines for assessing VSLs:

Guideline (1) – Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance

Compare the VSLs to any prior levels of non-compliance and avoid significant changes that may encourage a lower level of compliance than was required when levels of non-compliance were used.

Guideline (2) – Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties

A violation of a "binary" type requirement must be a "Severe" VSL.

Do not use ambiguous terms such as "minor" and "significant" to describe noncompliant performance.

Guideline (3) – Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement

VSLs should not expand on what is required in the requirement.

Guideline (4) – Violation Severity Level Assignment Should Be Based on a Single Violation, Not on a Cumulative Number of Violations

Unless otherwise stated in the requirement, each instance of non-compliance with a requirement is a separate violation. Section 4 of the Sanction Guidelines states that assessing penalties on a per violation per day basis is the "default" for penalty calculations.

VRF Justifications for CIP-012-1, Requirement R1	
Proposed VRF	**Medium**
NERC VRF Discussion	A VRF of Medium was assigned to this requirement. Cyber security plans enable effective implementation of the CIP standard's requirements to mitigate the risk of the unauthorized disclosure or modification of data used for Real-time Assessments and Real-time monitoring while being transmitted between Control Centers.
FERC VRF G1 Discussion Guideline 1- Consistency with Blackout Report	N/A
FERC VRF G2 Discussion Guideline 2- Consistency within a Reliability Standard	N/A
FERC VRF G3 Discussion Guideline 3- Consistency among Reliability Standards	The requirement complements CIP-005-1, Requirement R1, CIP-006-6, Requirement R1, and CIP-007-6, Requirement R1 which are related to security of networks and communications components. The proposed VRF is consistent with these related requirements.
FERC VRF G4 Discussion Guideline 4- Consistency with NERC Definitions of VRFs	Failure to have a cyber security plan would not, under Emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.
FERC VRF G5 Discussion	N/A

VRF Justifications for CIP-012-1, Requirement R1	
Proposed VRF	**Medium**
Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation	

VSLs for CIP-012-1, Requirement R1			
Lower	**Moderate**	**High**	**Severe**
N/A	The Responsible Entity documented its plan(s) but failed to include one of the applicable Parts of the plan as specified in Requirement R1.	The Responsible Entity documented its plan(s) but failed to include two of the applicable Parts of the plan as specified in Requirement R1.	The Responsible Entity failed to document plan(s) for Requirement R1; Or The Responsible Entity failed to implement any Part of its plan(s) for Requirement R1, except under CIP Exceptional Circumstances.

VSL Justifications for CIP-012-1 Requirements R1	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The requirement is new. Therefore, the proposed VSL does not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The requirement is for the Responsible Entity to implement one or more documented plan(s) as specified in Requirement R1. The moderate VSL addresses where the Responsible Entity documented its plan(s) but failed to include one of the applicable parts of the plan as specified in Requirement R1. The high VSL addresses where the Responsible Entity documented its plan(s) but failed to include two of the applicable parts of the plan as specified in Requirement R1. The severe VSL addresses where the Responsible Entity failed to document plan(s) for Requirement R1, or where the Responsible Entity failed to implement plan(s) for Requirement R1.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL uses the same terminology as used in the associated requirement and is, therefore, consistent with the requirement.

FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Each VSL is based on a single violation and not cumulative violations.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Violation Risk Factor and Violation Severity Level Justifications

Project 2016-02 Modifications to CIP Standards

This document provides the standard drafting team's (SDT's) justification for assignment of violation risk factors (VRFs) and violation severity levels (VSLs) for each requirement in **CIP-012-1**. Each requirement is assigned a VRF and a VSL. These elements support the determination of an initial value range for the Base Penalty Amount regarding violations of requirements in FERC-approved Reliability Standards, as defined in the Electric Reliability Organizations (ERO) Sanction Guidelines. The SDT applied the following NERC criteria and FERC Guidelines when developing the VRFs and VSLs for the requirements.

NERC Criteria for Violation Risk Factors

High Risk Requirement

A requirement that, if violated, could directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures, or could hinder restoration to a normal condition.

Medium Risk Requirement

A requirement that, if violated, could directly affect the electrical state or the capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System. However, violation of a medium risk requirement is unlikely to lead to Bulk Electric System instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System. However, violation of a medium risk requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to Bulk Electric System instability, separation, or cascading failures, nor to hinder restoration to a normal condition.

Lower Risk Requirement
A requirement that is administrative in nature and a requirement that, if violated, would not be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System; or, a requirement that is administrative in nature and a requirement in a planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.

FERC Guidelines for Violation Risk Factors

Guideline (1) – Consistency with the Conclusions of the Final Blackout Report

FERC seeks to ensure that VRFs assigned to Requirements of Reliability Standards in these identified areas appropriately reflect their historical critical impact on the reliability of the Bulk-Power System. In the VSL Order, FERC listed critical areas (from the Final Blackout Report) where violations could severely affect the reliability of the Bulk-Power System:

- Emergency operations
- Vegetation management
- Operator personnel training
- Protection systems and their coordination
- Operating tools and backup facilities
- Reactive power and voltage control
- System modeling and data exchange
- Communication protocol and facilities
- Requirements to determine equipment ratings
- Synchronized data recorders
- Clearer criteria for operationally critical facilities
- Appropriate use of transmission loading relief.

Guideline (2) – Consistency within a Reliability Standard

FERC expects a rational connection between the sub-Requirement VRF assignments and the main Requirement VRF assignment.

Guideline (3) – Consistency among Reliability Standards

FERC expects the assignment of VRFs corresponding to Requirements that address similar reliability goals in different Reliability Standards would be treated comparably.

Guideline (4) – Consistency with NERC's Definition of the Violation Risk Factor Level

Guideline (4) was developed to evaluate whether the assignment of a particular VRF level conforms to NERC's definition of that risk level.

Guideline (5) – Treatment of Requirements that Co-mingle More Than One Obligation

Where a single Requirement co-mingles a higher risk reliability objective and a lesser risk reliability objective, the VRF assignment for such Requirements must not be watered down to reflect the lower risk level associated with the less important objective of the Reliability Standard.

NERC Criteria for Violation Severity Levels

VSLs define the degree to which compliance with a requirement was not achieved. Each requirement must have at least one VSL. While it is preferable to have four VSLs for each requirement, some requirements do not have multiple "degrees" of noncompliant performance and may have only one, two, or three VSLs.

VSLs should be based on NERC's overarching criteria shown in the table below:

Lower VSL	Moderate VSL	High VSL	Severe VSL
The performance or product measured almost meets the full intent of the requirement.	The performance or product measured meets the majority of the intent of the requirement.	The performance or product measured does not meet the majority of the intent of the requirement, but does meet some of the intent.	The performance or product measured does not substantively meet the intent of the requirement.

FERC Order of Violation Severity Levels

The FERC VSL guidelines are presented below, followed by an analysis of whether the VSLs proposed for each requirement in the standard meet the FERC Guidelines for assessing VSLs:

Guideline (1) – Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance

Compare the VSLs to any prior levels of non-compliance and avoid significant changes that may encourage a lower level of compliance than was required when levels of non-compliance were used.

Guideline (2) – Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties

A violation of a "binary" type requirement must be a "Severe" VSL.

Do not use ambiguous terms such as "minor" and "significant" to describe noncompliant performance.

Guideline (3) – Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement

VSLs should not expand on what is required in the requirement.

Guideline (4) – Violation Severity Level Assignment Should Be Based on a Single Violation, Not on a Cumulative Number of Violations

Unless otherwise stated in the requirement, each instance of non-compliance with a requirement is a separate violation. Section 4 of the Sanction Guidelines states that assessing penalties on a per violation per day basis is the "default" for penalty calculations.

VRF Justifications for CIP-012-1, Requirement R1	
Proposed VRF	**Medium**
NERC VRF Discussion	A VRF of Medium was assigned to this requirement. Cyber security plans enable effective implementation of the CIP standard's requirements to mitigate the risk of the unauthorized disclosure or modification of data used for Real-time Assessments and Real-time monitoring while being transmitted between Control Centers.
FERC VRF G1 Discussion Guideline 1- Consistency with Blackout Report	N/A
FERC VRF G2 Discussion Guideline 2- Consistency within a Reliability Standard	N/A
FERC VRF G3 Discussion Guideline 3- Consistency among Reliability Standards	The requirement complements CIP-005-1, Requirement R1, CIP-006-6, Requirement R1, and CIP-007-6, Requirement R1 which are related to security of networks and communications components. The proposed VRF is consistent with these related requirements.
FERC VRF G4 Discussion Guideline 4- Consistency with NERC Definitions of VRFs	Failure to have a cyber security plan would not, under Emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.
FERC VRF G5 Discussion	N/A

VRF Justifications for CIP-012-1, Requirement R1	
Proposed VRF	**Medium**
Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation	

VSLs for CIP-012-1, Requirement R1			
Lower	**Moderate**	**High**	**Severe**
N/A	The Responsible Entity documented its plan(s) but failed to include one of the applicable ~~p~~Parts of the plan as specified in Requirement R1.	The Responsible Entity documented its plan(s) but failed to include two of the applicable ~~p~~Parts of the plan as specified in Requirement R1.	The Responsible Entity failed to document plan(s) for Requirement R1; Or The Responsible Entity failed to implement any Part of its plan(s) for Requirement R1, except under CIP Exceptional Circumstances.

VSL Justifications for CIP-012-1 Requirements R1	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The requirement is new. Therefore, the proposed VSL does not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The requirement is for the Responsible Entity to implement one or more documented plan(s) as specified in Requirement R1. The moderate VSL addresses where the Responsible Entity documented its plan(s) but failed to include one of the applicable parts of the plan as specified in Requirement R1. The high VSL addresses where the Responsible Entity documented its plan(s) but failed to include two of the applicable parts of the plan as specified in Requirement R1. The severe VSL addresses where the Responsible Entity failed to document plan(s) for Requirement R1, or where the Responsible Entity failed to implement plan(s) for Requirement R1.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL uses the same terminology as used in the associated requirement and is, therefore, consistent with the requirement.

FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Each VSL is based on a single violation and not cumulative violations.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DRAFT

Cyber Security – Communications between Control Centers

Technical Rationale and Justification for Reliability Standard CIP-012-1

May 2018

RELIABILITY | ACCOUNTABILITY



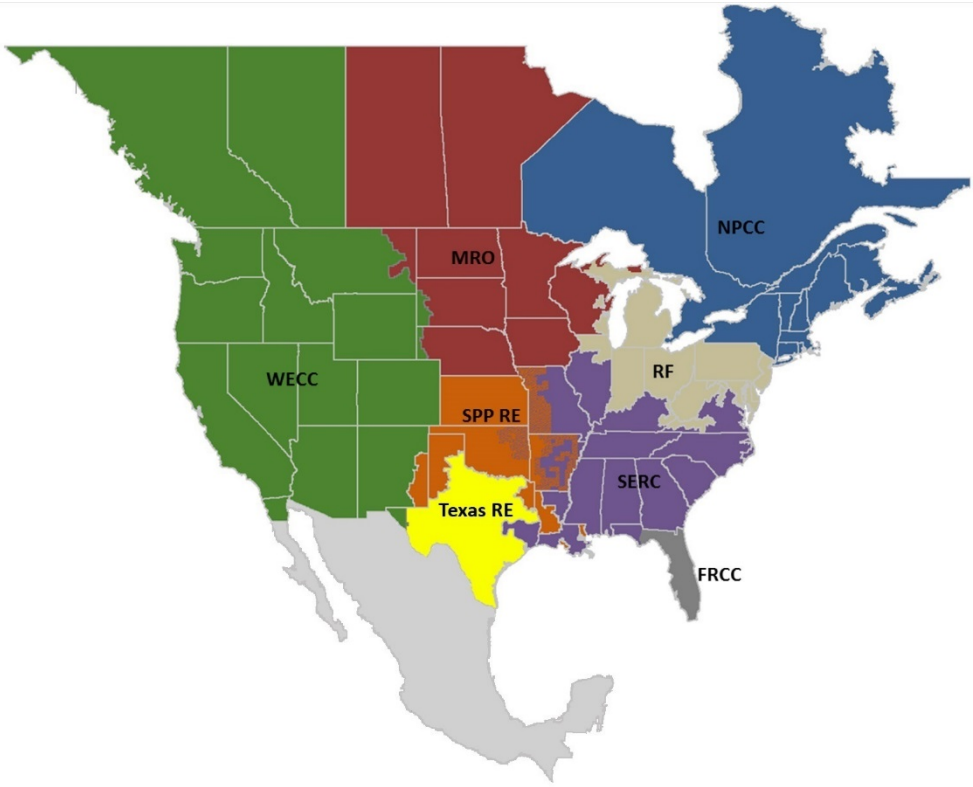

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Preface

The vision for the Electric Reliability Organization (ERO) Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the eight Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

The North American BPS is divided into eight RE boundaries as shown in the map and corresponding table below.



The North American BPS is divided into eight RE boundaries. The highlighted areas denote overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.

FRCC	Florida Reliability Coordinating Council
MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
SPP RE	Southwest Power Pool Regional Entity
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-012-1. It will provide stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. It also contains information on the SDT's intent in drafting the requirements. This Technical Rationale and Justification for CIP-012-1 is not a Reliability Standard and should not be considered mandatory and enforceable.

On January 21, 2016, the Federal Energy Regulatory Commission (FERC or Commission) issued Order No. 822, approving seven Critical Infrastructure Protection (CIP) Reliability Standards and new or modified terms in the Glossary of Terms Used in NERC Reliability Standards, and directing modifications to the CIP Reliability Standards. Among others, the Commission directed the North American Electric Reliability Corporation (NERC) to "develop modifications to the CIP Reliability Standards to require Responsible Entities[1] to implement controls to protect, at a minimum, communication links and sensitive bulk electric system data communicated between bulk electric system Control Centers in a manner that is appropriately tailored to address the risks posed to the bulk electric system by the assets being protected (i.e., high, medium, or low impact)." (Order 822, Paragraph 53)

In response to the directive in Order No. 822, the Project 2016-02 standard drafting team (SDT) drafted Reliability Standard CIP-012-1 to require Responsible Entities to implement controls to protect sensitive Bulk Electric System (BES) data and communications links between BES Control Centers. Due to the sensitivity of the data being communicated between Control Centers, as defined in the Glossary of Terms Used in NERC Reliability Standards, the standard applies to all impact levels (i.e., high, medium, or low impact).

Although the Commission directed NERC to develop modifications to CIP-006, the SDT determined that modifications to CIP-006 would not be appropriate. There are differences between the plan(s) required to be developed and implemented for CIP-012-1 and the protection required in CIP-006-6 Requirement R1 Part 1.10. CIP-012-1 Requirements R1 and R2 protect the applicable data during transmission between two separate Control Centers. CIP-006 Requirement R1 Part 1.10 protects nonprogrammable communication components within an Electronic Security Perimeter (ESP) but outside of a Physical Security Perimeter (PSP). The transmission of applicable data between Control Centers takes place outside of an ESP. Therefore, the protection contained in CIP-006-6 Requirement R1 Part 1.10 does not apply.

The SDT drafted requirements to provide Responsible Entities the latitude to protect the communication links, the data, or both to satisfy the security objective consistent with the capabilities of the Responsible Entity's operational environment.

CIP-012 Exemption (4.2.3) for certain Control Centers

As the SDT drafted CIP-012, it became aware of certain generating plant or Transmission substation situations where such field assets could be dual-classified as Control Centers based on the current Control Center definition. However, their communications to their normal BA or TOP Control Center are not the type of communications that are the intended scope of CIP-012 as they do not differ from any other generating plant or substation. The SDT wrote an exemption (Section 4.2.3 within CIP-012) for this particular scenario which is described in further detail below.

[1] As used in the CIP Standards, a Responsible Entity refers to the registered entities subject to the CIP Standards.

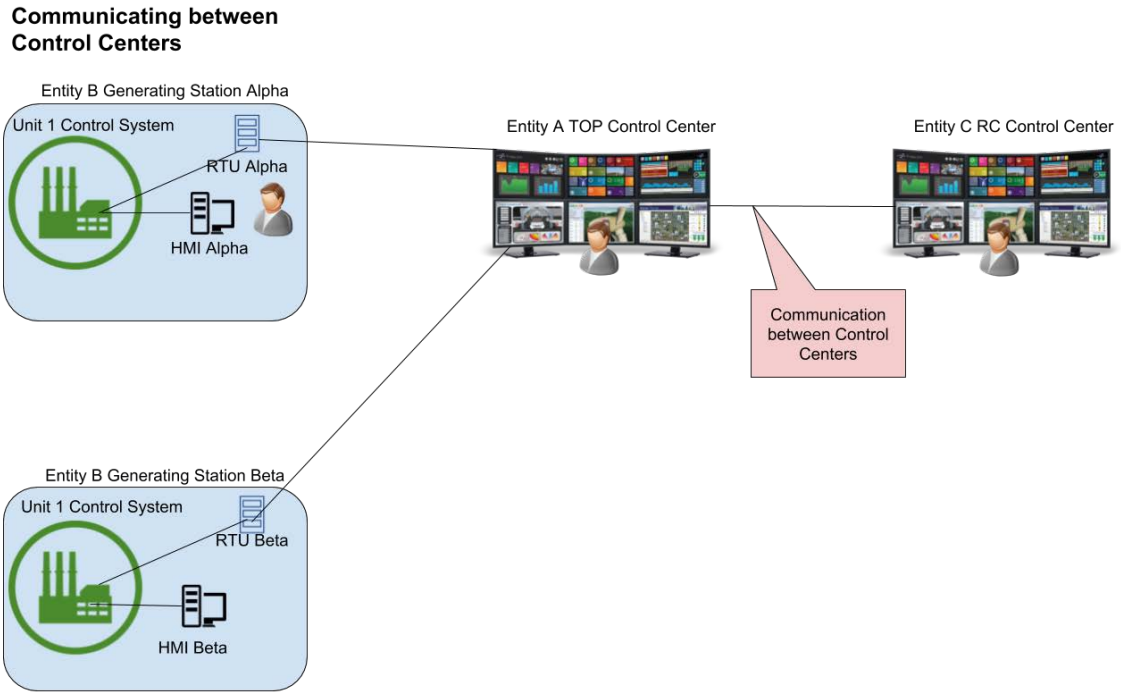


Figure 1

Figure 1 above pictures a typical scenario with two Control Centers communicating (in this instance Entity C's RC Control Center and Entity A's TOP Control Center). The communication between them is the intended scope of CIP-012's requirements if it meets the types of data inclusions and exclusions within the standard. The TOP Control Center is communicating with an RTU at two of Entity B's generating plants (Stations Alpha and Beta) and those RTU's are gathering information from each generating unit's control system. Each generating unit at each plant has an HMI (Human/Machine Interface; an operator workstation) that the local personnel use to operate their respective units.

Entity B decides that the generating unit at Station Beta, a small peaking facility, will only have an operator on site during the day and the operator at Station Alpha should be able to remotely start the unit at Station Beta if necessary.

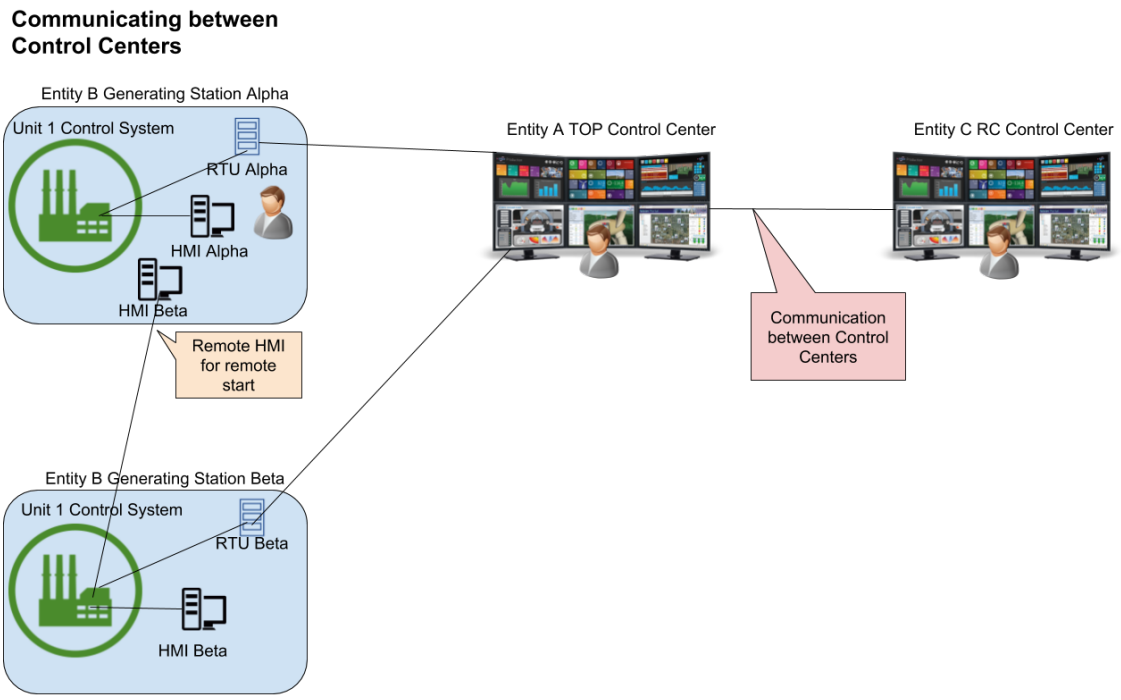


Figure 2

In Figure 2, Entity B installs a dedicated communications circuit from the control system on Station Beta's control system and puts a dedicated HMI at Station Alpha the operator can use. Station Alpha is now "one or more facilities hosting operating personnel that monitor and control the BES in real time to perform the reliability tasks of…a Generator Operator for generation Facilities at two or more locations." It can now be dual-classified not only as a generation resource but also as a Control Center.

The communications to the TOP and RC Control Centers from Figure 1 have not changed at all. No new cyber systems are in place that can impact multiple units. No cyber systems have been added performing Control Center functions. No additional risk from cyber systems has been added. The only thing that has changed is an HMI for Station Beta has been moved within close physical proximity to an HMI for Station Alpha.

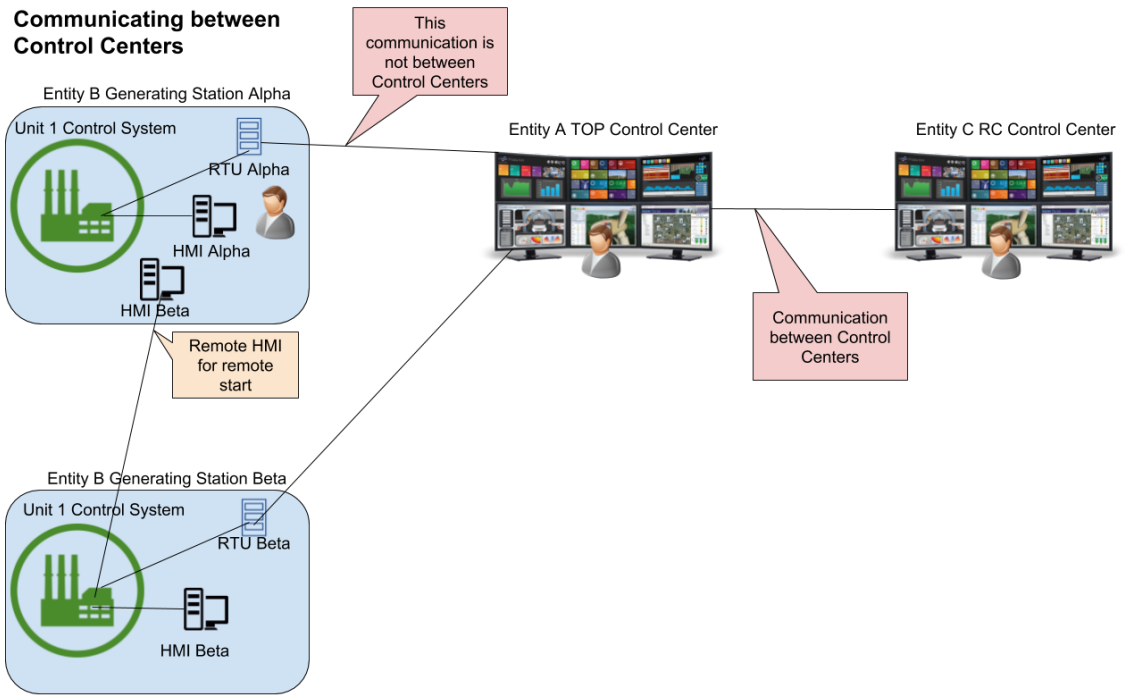


Figure 3

The SDT realized how this suddenly makes the communication noted in Figure 3 between Station Alpha and Entity A's TOP Control Center subject to CIP-012 although nothing has changed between them. There is no new risk involved. Two HMI's have been moved into the same room and suddenly a new NERC CIP standard applies to two entities.

This is an anamoly of the current Control Center definition defining a facility, room, or building from which something can be done without regard to how its done or with what systems. This is a generation specific example, but the SDT can envision substations with an HMI or protective relay that "operating personnel" within the substation could use to impact an adjacent substation. The SDT realizes that in the criteria for TO's and GOP's the "two or more geographic locations" is not a precise enough filter for capturing what a Control Center truly is. The SDT's attempts to address this issue by clarifying the definition of Control Center pointed out larger issues that are not within the SDT's SAR to address at this time. Therefore the SDT is handling the issue this creates for CIP-012 by the 4.2.3 exemption within the CIP-012 standard which reads:

> 4.2.3. A Control Center at a generation resource or Transmission station or substation that transmits to another Control Center Real-time Assessment or Real-time monitoring data pertaining only to the generation resource or Transmission station or substation at which the transmitting Control Center is located.

The intent of this exemption is to exclude the normal RTU-style communication from a field asset about that field asset's status from CIP-012. Throughout this scenario or others like it, that communication has not changed and is still the same data pertaining only to the single location. The SDT recognizes that this communication is not the intent of the standard for protecting communications between Control Centers and this type of communications can be using older legacy communication technology and protocols.

Requirement R1

R1. The Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring data while being transmitted between any applicable Control Centers. The Responsible Entity is not required to include oral communications in its plan. The plan shall include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1 *Identification of security protection used to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring while being transmitted between Control Centers;*

1.2 *Identification of where the Responsible Entity applied security protection for transmitting Real-time Assessment and Real-time monitoring data between Control Centers; and*

1.3 *If he Control Centers are owned or operated by different Responsible Entities,identify the responsibilities of each Responsible Entity for applying security protection to the transmission of Real-time Assessment and Real-time monitoring data between those Control Centers.*

General Considerations for Requirement R1

Requirement R1 focuses on implementing a documented plan to protect information that is critical to the Real-time operations of the Bulk Electric System while in transit between applicable Control Centers. The SDT does not intend for the listed order of the three requirement parts to convey any sequence or significance.

Overview of confidentiality and integrity

The SDT drafted CIP-012-1 to address confidentiality and integrity of Real-time Assessment and Real-time monitoring data. This is accomplished by drafting the requirement to mitigate the risk of unauthorized disclosure (confidentiality) or modification (integrity). For this Standard, the SDT relied on the definitions of confidentiality and integrity as defined by National Institute of Standards and Technology (NIST):

- Confidentiality is defined as, "Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information."[2]
- Integrity is defined as, "Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity."[3]

The SDT asserts that the availability of this data is already required by the performance obligation of the Operating and Planning Reliability Standards. The SDT drafted CIP-012 to address the data while being transmitted. The SDT maintains that this data resides within BES Cyber Systems, and while at rest is protected by CIP-003 through CIP-011.

Alignment with IRO and TOP standards

The SDT recognized the FERC reference to additional Reliability Standards and the responsibilities to protect the applicable data in accordance with NERC Reliability Standards TOP-003 and IRO-010. The SDT used these references to drive the identification of sensitive BES data and chose to base the CIP-012 requirements on the Real-time data specification elements in these standards. This approach provides consistent scoping of identified data, and does not require each entity to devise its own list or inventory of this data. Many entities are required to provide this data under agreements executed with their RC, BA or TOP. The SDT asserts that typically the RC, BA or TOP will identify

[2] NIST Special Publication 800-53A, Revision 4, page B-3
[3] NIST Special Publication 800-53A, Revision 4, page B-6

all data requiring protection for CIP-012-1 through the TOP-003 and IRO-010 Reliability Standards. However, the SDT noted that there may be special instances during which Real-time Assessment or Real-time monitoring data is not identified by the RC, BA, or TOP. This would include data that may be exchanged between a Responsible Entity's primary and backup Control Center.

Identification of Where Security Protection is Applied by the Responsible Entity

The SDT noted the need for a Responsible Entity to identify where it will apply protection for applicable data. The SDT did not specify the location where CIP-012 security protection must be applied to provide latitude for Responsible Entities to implement the security controls in a manner best fitting their individual circumstances. This latitude ensures entities can still take advantage of security measures, such as deep packet inspection implemented at or near the EAP when ESPs are present, while maintaining the capability to protect the applicable data being transmitted between Control Centers.

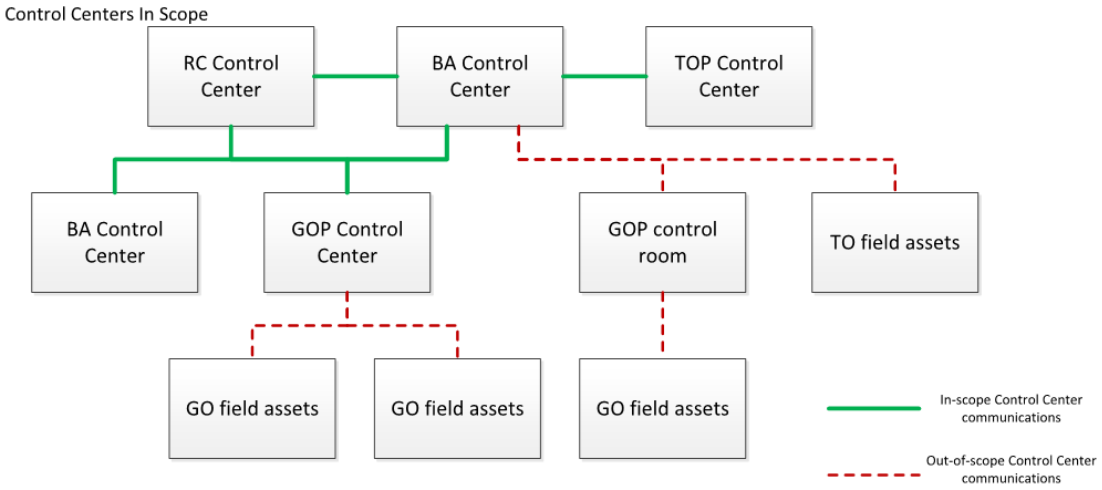
The SDT also recognizes that CIP-012 security protection may be applied to a Cyber Asset that is not an identified BES Cyber Asset or EACMS. The identification of the Cyber Asset as the location where security protection is applied does not expand the scope of Cyber Assets identified as applicable under Cyber Security Standards CIP-002 through CIP-011.

The SDT understands that in data exchanges between Control Centers, a single entity may not be responsible for both ends of the communication link. The SDT intends for a Responsible Entity to identify only where it applied security protection. The Responsible Entity should not be held accountable for identifying where a neighboring entity applied security protection at the neighboring entity's facility. A Responsible Entity, however, may decide to take responsibility for both ends of a communication link. For example, it may place a router in a neighboring entity's data center. In a scenario like this, where a Responsible Entity has taken responsibility for applying security protection on both ends of the communication link, the Responsible Entity should identify where it applied security protection at both ends of the link. The SDT intends for there to be alignment between the identification of where security protection is applied in CIP-012 R1, Part 1.2 and the identification of Responsible Entity responsibilities in CIP-012 R1, Part 1.3.

Control Center Ownership

The requirements address protection for Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers owned by a single Responsible Entity. They also cover the applicable data transmitted between Control Centers owned by two or more separate Responsible Entities. Unlike protection between a single Responsible Entity's Control Centers, applying protection between Control Centers owned by more than one Responsible Entity requires additional coordination. The requirements do not explicitly require formal agreements between Responsible Entities partnering for protection of applicable data. It is strongly recommended, however, that these partnering entities develop agreements, or use existing ones, to define responsibilities to ensure the security objective is met. An example noted in FERC Order No. 822 Paragraph 59 is, "if several registered entities have joint responsibility for a cryptographic key management system used between their respective Control Centers, they should have the prerogative to come to a consensus on which organization administers that particular key management system."

As an example, the reference model below shows some of the data transmissions between Control Centers that a Responsible Entity should consider to be in-scope. The example does not include all possible scenarios. The solid green lines are in-scope communications. The dashed red lines are out-of-scope communications.



This reference model is an example and does not include all possible scenarios.

References

Here are several references to assist entities in developing plan(s) for protection of communication links:

- NIST Special Publication 800-53A, Revision 4: Security and Privacy Controls for Federal Information Systems and Organizations
- NIST Special Publication 800-82: Guide to Industrial Control Systems (ICS) Security
- NIST Special Publication 800-175B: Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms
- NIST Special Publication 800-47: Security Guide for Interconnecting Information Technology Systems

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DRAFT

Cyber Security – Communications between Control Centers

Technical Rationale and Justification for Reliability Standard CIP-012-1

~~March~~ May 2018

RELIABILITY | ACCOUNTABILITY



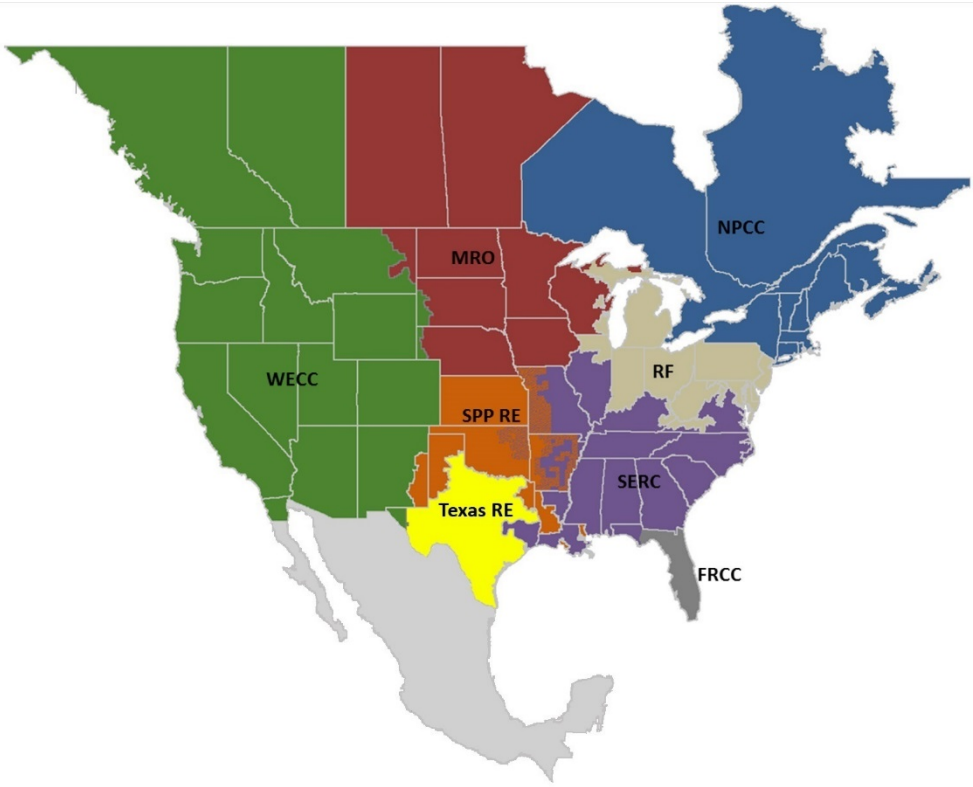

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Preface

The vision for the Electric Reliability Organization (ERO) Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the eight Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

The North American BPS is divided into eight RE boundaries as shown in the map and corresponding table below.



The North American BPS is divided into eight RE boundaries. The highlighted areas denote overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.

FRCC	Florida Reliability Coordinating Council
MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
SPP RE	Southwest Power Pool Regional Entity
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-012-1. It will provide stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. It also contains information on the SDT's intent in drafting the requirements. This Technical Rationale and Justification for CIP-012-1 is not a Reliability Standard and should not be considered mandatory and enforceable.

On January 21, 2016, the Federal Energy Regulatory Commission (FERC or Commission) issued Order No. 822, approving seven Critical Infrastructure Protection (CIP) Reliability Standards and new or modified terms in the Glossary of Terms Used in NERC Reliability Standards, and directing modifications to the CIP Reliability Standards. Among others, the Commission directed the North American Electric Reliability Corporation (NERC) to "develop modifications to the CIP Reliability Standards to require Responsible Entities[1] to implement controls to protect, at a minimum, communication links and sensitive bulk electric system data communicated between bulk electric system Control Centers in a manner that is appropriately tailored to address the risks posed to the bulk electric system by the assets being protected (i.e., high, medium, or low impact)." (Order 822, Paragraph 53)

In response to the directive in Order No. 822, the Project 2016-02 standard drafting team (SDT) drafted Reliability Standard CIP-012-1 to require Responsible Entities to implement controls to protect sensitive Bulk Electric System (BES) data and communications links between BES Control Centers. Due to the sensitivity of the data being communicated between Control Centers, as defined in the Glossary of Terms Used in NERC Reliability Standards, the standard applies to all impact levels (i.e., high, medium, or low impact).

Although the Commission directed NERC to develop modifications to CIP-006, the SDT determined that modifications to CIP-006 would not be appropriate. There are differences between the plan(s) required to be developed and implemented for CIP-012-1 and the protection required in CIP-006-6 Requirement R1 Part 1.10. CIP-012-1 Requirements R1 and R2 protect the applicable data during transmission between two separate Control Centers. CIP-006 Requirement R1 Part 1.10 protects nonprogrammable communication components within an Electronic Security Perimeter (ESP) but outside of a Physical Security Perimeter (PSP). The transmission of applicable data between Control Centers takes place outside of an ESP. Therefore, the protection contained in CIP-006-6 Requirement R1 Part 1.10 does not apply.

The SDT drafted requirements to provide Responsible Entities the latitude to protect the communication links, the data, or both to satisfy the security objective consistent with the capabilities of the Responsible Entity's operational environment.

CIP-012 Exemption (4.2.3) for certain Control Centers

As the SDT drafted CIP-012, it became aware of certain generating plant or Transmission substation situations where such field assets could be dual-classified as Control Centers based on the current Control Center definition. However, their communications to their normal BA or TOP Control Center are not the type of communications that are the intended scope of CIP-012 as they do not differ from any other generating plant or substation. The SDT wrote an exemption (Section 4.2.3 within CIP-012) for this particular scenario which is described in further detail below.

[1] As used in the CIP Standards, a Responsible Entity refers to the registered entities subject to the CIP Standards.

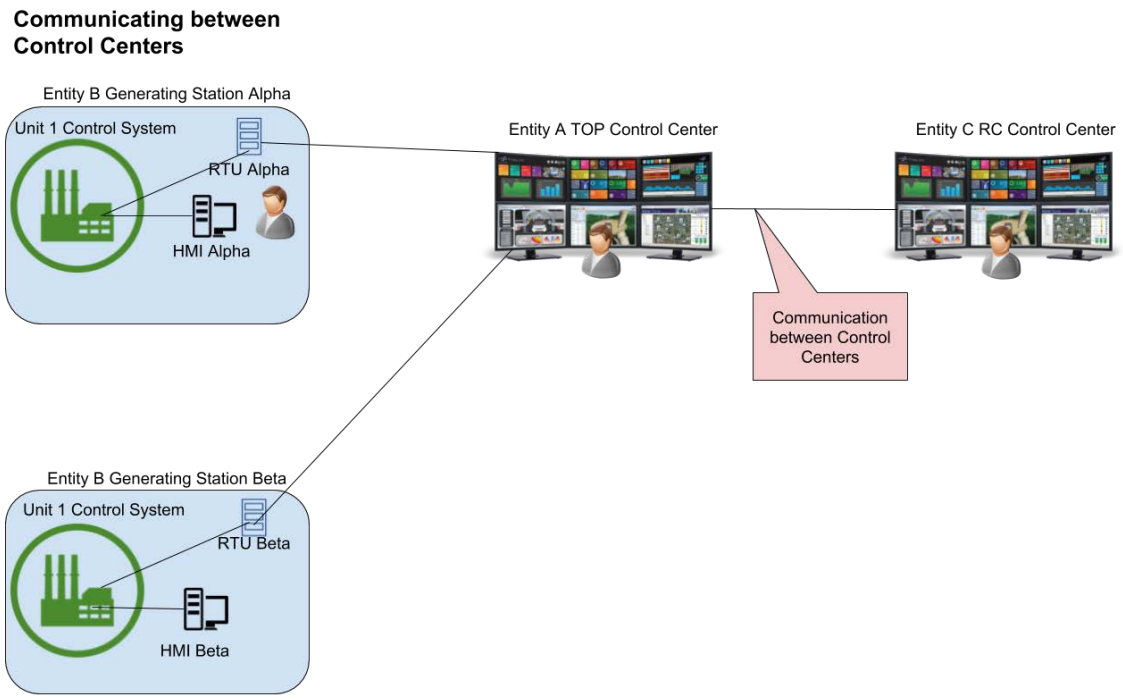


Figure 1

Figure 1 above pictures a typical scenario with two Control Centers communicating (in this instance Entity C's RC Control Center and Entity A's TOP Control Center). The communication between them is the intended scope of CIP-012's requirements if it meets the types of data inclusions and exclusions within the standard. The TOP Control Center is communicating with an RTU at two of Entity B's generating plants (Stations Alpha and Beta) and those RTU's are gathering information from each generating unit's control system. Each generating unit at each plant has an HMI (Human/Machine Interface; an operator workstation) that the local personnel use to operate their respective units.

Entity B decides that the generating unit at Station Beta, a small peaking facility, will only have an operator on site during the day and the operator at Station Alpha should be able to remotely start the unit at Station Beta if necessary.

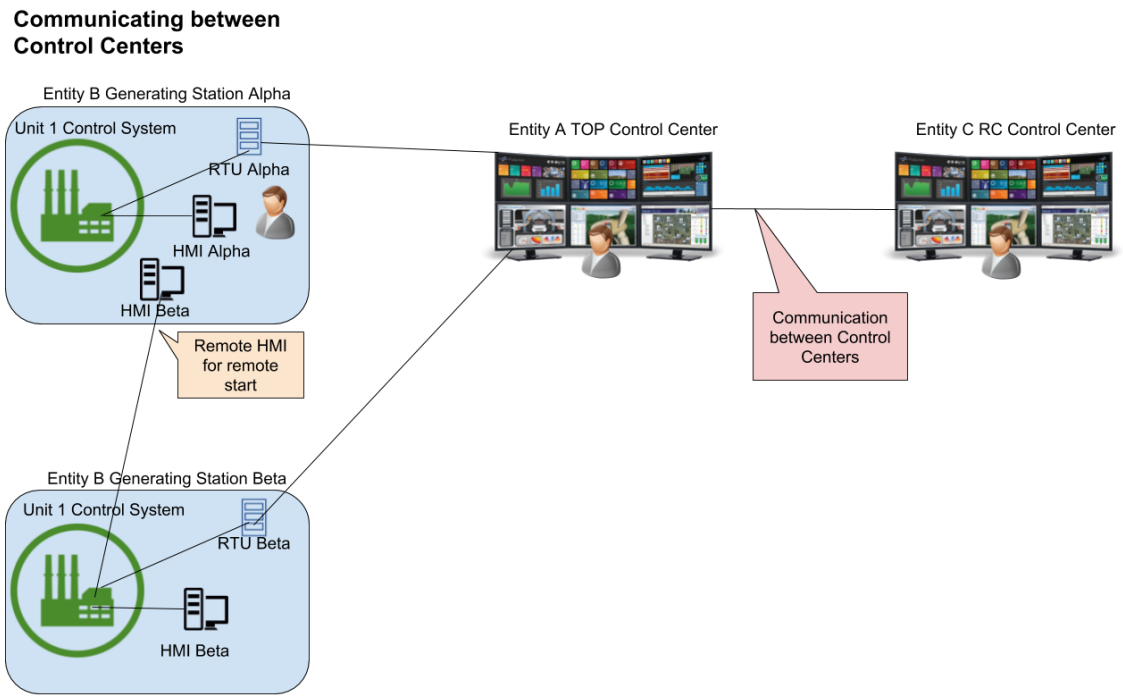


Figure 2

In Figure 2, Entity B installs a dedicated communications circuit from the control system on Station Beta's control system and puts a dedicated HMI at Station Alpha the operator can use. Station Alpha is now "one or more facilities hosting operating personnel that monitor and control the BES in real time to perform the reliability tasks of…a Generator Operator for generation Facilities at two or more locations." It can now be dual-classified not only as a generation resource but also as a Control Center.

The communications to the TOP and RC Control Centers from Figure 1 have not changed at all. –No new cyber systems are in place that can impact multiple units. -No cyber systems have been added performing Control Center functions. No additional risk from cyber systems has been added. -The only thing that has changed is an HMI for Station Beta has been moved within close physical proximity to an HMI for Station Alpha.

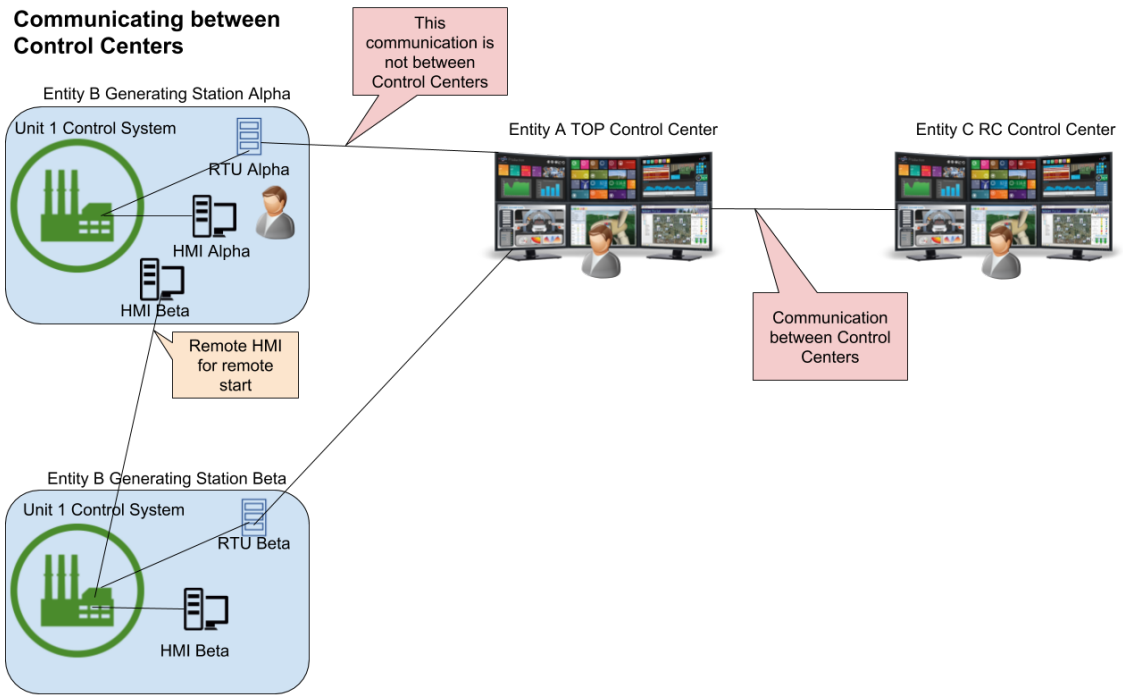


Figure 3

The SDT realized how this suddenly makes the communication noted in Figure 3 between Station Alpha and Entity A's TOP Control Center subject to CIP-012 although nothing has changed between them. —There is no new risk involved. -Two HMI's have been moved into the same room and suddenly a new NERC CIP standard applies to two entities.

This is an anamoly of the current Control Center definition defining a facility, room, or building from which something can be done without regard to how its done or with what systems. This is a generation specific example, but the SDT can envision substations with an HMI or protective relay that "operating personnel" within the substation could use to impact an adjacent substation. The SDT realizes that in the criteria for TO's and GOP's the "two or more geographic locations" is not a precise enough filter for capturing what a Control Center truly is. The SDT's attempts to address this issue by clarifying the definition of Control Center pointed out larger issues that are not within the SDT's SAR to address at this time. Therefore the SDT is handling the issue this creates for CIP-012 by the 4.2.3 exemption within the CIP-012 standard which reads:

> 4.2.3. ————A Control Center at a generation resource or Transmission station or substation that transmits to another Control Center Real-time Assessment or Real-time monitoring data pertaining only to the generation resource or Transmission station or substation at which the transmitting Control Center is located.
> ~~Control Centers located at a generation resource or Transmission station or substation that transmits Real-time Assessment and Real-time monitoring data to another Control Center and that data pertains only to the generation resource or Transmission station or substation at which the Control Center is located.~~

The intent of this exemption is to exclude the normal RTU-style communication from a field asset about that field asset's status from CIP-012. -Throughout this scenario or others like it, that communication has not changed and is still the same data pertaining only to the single location. -The SDT recognizes that this communication is not the

intent of the standard for protecting communications between Control Centers and this type of communications can be using older legacy communication technology and protocols.

Requirement R1

R1. The Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring data while being transmitted between any applicable Control Centers. ~~This requirement excludes oral communications.~~ The Responsible Entity is not required to include oral communications in its plan. ~~-~~The plan shall include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1 *Identification of security protection used to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring while being transmitted between Control Centers;*

1.2 *Identification of where the Responsible Entity applied security protection for transmitting Real-time Assessment and Real-time monitoring data between Control Centers; and*

1.3 *If he Control Centers are owned or operated by different Responsible Entities,identify the responsibilities of each Responsible Entity for applying security protection to the transmission of Real-time Assessment and Real-time monitoring data between those Control Centers.*

General Considerations for Requirement R1

Requirement R1 focuses on implementing a documented plan to protect information that is critical to the Real-time operations of the Bulk Electric System while in transit between applicable Control Centers. The SDT does not intend for the listed order of the three requirement parts to convey any sequence or significance.

Overview of confidentiality and integrity

The SDT drafted CIP-012-1 to address confidentiality and integrity of Real-time Assessment and Real-time monitoring data. This is accomplished by drafting the requirement to mitigate the risk of unauthorized disclosure (confidentiality) or modification (integrity). For this Standard, the SDT relied on the definitions of confidentiality and integrity as defined by National Institute of Standards and Technology (NIST):

- Confidentiality is defined as, "Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information."[2]
- Integrity is defined as, "Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity."[3]

The SDT asserts that the availability of this data is already required by the performance obligation of the Operating and Planning Reliability Standards. The SDT drafted CIP-012 to address the data while being transmitted. The SDT maintains that this data resides within BES Cyber Systems, and while at rest is protected by CIP-003 through CIP-011.

Alignment with IRO and TOP standards

The SDT recognized the FERC reference to additional Reliability Standards and the responsibilities to protect the applicable data in accordance with NERC Reliability Standards TOP-003 and IRO-010. The SDT used these references to drive the identification of sensitive BES data and chose to base the CIP-012 requirements on the Real-time data specification elements in these standards. This approach provides consistent scoping of identified data, and does not require each entity to devise its own list or inventory of this data. Many entities are required to provide this data

[2] NIST Special Publication 800-53A, Revision 4, page B-3
[3] NIST Special Publication 800-53A, Revision 4, page B-6

under agreements executed with their RC, BA or TOP. The SDT asserts that typically the RC, BA or TOP will identify all data requiring protection for CIP-012-1 through the TOP-003 and IRO-010 Reliability Standards. However, the SDT noted that there may be special instances during which Real-time Assessment or Real-time ~~Monitoring~~ monitoring data is not identified by the RC, BA, or TOP. This would include data that may be exchanged between a Responsible Entity's primary and backup Control Center.

Identification of Where Security Protection is Applied by the Responsible Entity

The SDT noted the need for a Responsible Entity to identify where it will apply protection for applicable data. The SDT did not specify the location where CIP-012 security protection must be applied to provide latitude for Responsible Entities to implement the security controls in a manner best fitting their individual circumstances. This latitude ensures entities can still take advantage of security measures, such as deep packet inspection implemented at or near the EAP when ESPs are present, while maintaining the capability to protect the applicable data being transmitted between Control Centers.

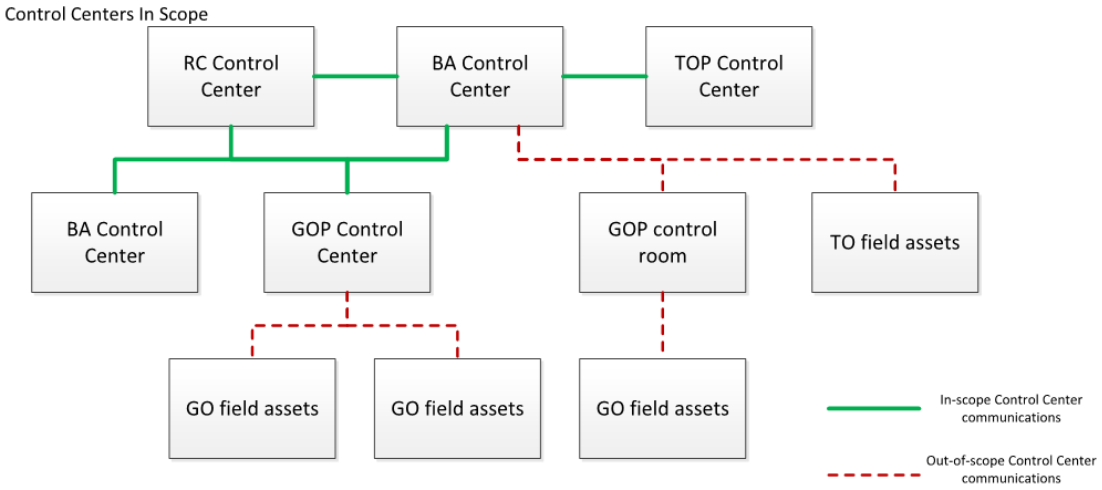
The SDT also recognizes that CIP-012 security protection may be applied to a Cyber Asset that is not an identified BES Cyber Asset or EACMS. The identification of the Cyber Asset as the location where security protection is applied does not expand the scope of Cyber Assets identified as applicable under Cyber Security Standards CIP-002 through CIP-011.

The SDT understands that in data exchanges between Control Centers, a single entity may not be responsible for both ends of the communication link. The SDT intends for a Responsible Entity to identify only where it applied security protection. The Responsible Entity should not be held accountable for identifying where a neighboring entity applied security protection at the neighboring entity's facility. A Responsible Entity, however, may decide to take responsibility for both ends of a communication link. For example, it may place a router in a neighboring entity's data center. In a scenario like this, where a Responsible Entity has taken responsibility for applying security protection on both ends of the communication link, the Responsible Entity should identify where it applied security protection at both ends of the link. The SDT intends for there to be alignment between the identification of where security protection is applied in CIP-012 R1, Part 1.2 and the identification of Responsible Entity responsibilities in CIP-012 R1, Part 1.3.

Control Center Ownership

The requirements address protection for Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers owned by a single Responsible Entity. They also cover the applicable data transmitted between Control Centers owned by two or more separate Responsible Entities. Unlike protection between a single Responsible Entity's Control Centers, applying protection between Control Centers owned by more than one Responsible Entity requires additional coordination. The requirements do not explicitly require formal agreements between Responsible Entities partnering for protection of applicable data. It is strongly recommended, however, that these partnering entities develop agreements, or use existing ones, to define responsibilities to ensure the security objective is met. An example noted in FERC Order No. 822 Paragraph 59 is, "if several registered entities have joint responsibility for a cryptographic key management system used between their respective Control Centers, they should have the prerogative to come to a consensus on which organization administers that particular key management system."

As an example, the reference model below shows some of the data transmissions between Control Centers that a Responsible Entity should consider to be in-scope. The example does not include all possible scenarios. The solid green lines are in-scope communications. The dashed red lines are out-of-scope communications.



This reference model is an example and does not include all possible scenarios.

References

Here are several references to assist entities in developing plan(s) for protection of communication links:

- NIST Special Publication 800-53A, Revision 4: Security and Privacy Controls for Federal Information Systems and Organizations
- NIST Special Publication 800-82: Guide to Industrial Control Systems (ICS) Security
- NIST Special Publication 800-175B: Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms
- NIST Special Publication 800-47: Security Guide for Interconnecting Information Technology Systems

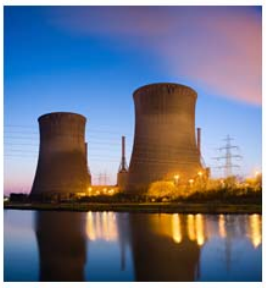
NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DRAFT

Cyber Security – Communications Between Control Centers

Implementation Guidance for CIP-012-1

RELIABILITY | ACCOUNTABILITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Introduction

The Project 2016-02 SDT drafted this Implementation Guidance to provide example approaches for compliance with CIP-012-1. Implementation Guidance does not prescribe the only approach, but highlights one or more approaches that would be effective in achieving compliance with the standard. Because Implementation Guidance only provides examples, entities may choose alternative approaches that better fit their individual situations[1].

Responsible Entities may find it useful to consider this Implementation Guidance document along with the additional context and background provided in the SDT-developed Technical Rationale and Justification for CIP-012-1 document.

Background

The Commission issued Order No. 822 on January 21, 2016. Order 822 approving seven CIP Reliability Standards and new or modified definitions, and directed modifications be made to the CIP Reliability Standards. Among other items, the Commission directed NERC to "develop modifications to the CIP Reliability Standards to require responsible entities to implement controls to protect, at a minimum, communication links and sensitive bulk electric system data communicated between bulk electric system Control Centers in a manner that is appropriately tailored to address the risks posed to the bulk electric system by the assets being protected (i.e., high, medium, or low impact)." (Order 822, Paragraph 53)

In response to the directive in Order No. 822, the Project 2016-02 standard drafting team (SDT) drafted Reliability Standard CIP-012-1 to require Responsible Entities to implement controls to protect sensitive Bulk Electric System (BES) data and communications links between BES Control Centers. Due to the sensitivity of the data being communicated between Control Centers, the standard applies to all impact levels (i.e., high, medium, or low impact).

The SDT drafted requirements to provide Responsible Entities the latitude to protect the communication links, the data, or both, to satisfy the security objective consistent with the capabilities of the Responsible Entity's operational environment.

[1] NERC's Compliance Guidance Policy

Requirements

R1. *The Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring data while being transmitted between any applicable Control Centers. The Responsible Entity is not required to include oral communications in its plan. The plan shall include: [Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. Identification of security protection used to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers;

1.2. Identification of where the Responsible Entity applied security protection for transmitting Real-time Assessment and Real-time monitoring and control data between Control Centers; and

1.3. If the Control Centers are owned or operated by different Responsible Entities, identify the responsibilities of each Responsible Entity for applying security protection to the transmission of Real-time Assessment and Real-time monitoring data between those Control Centers.

General Considerations

Plan Development

As noted in the Technical Rationale and Justification for CIP-012-1, the focus of Requirement R1 is implementing a documented plan to protect information that is critical to the real-time operations of the Bulk Electric System while in transit between applicable Control Centers. The number of plan(s) and their content may vary depending on a Responsible Entity's management structure and operating conditions. The Responsible Entity may document as many plans as necessary to meet its needs. For instance, a Responsible Entity may choose to document one plan per Control Center or choose an all-inclusive, single plan for its Control Center communication environment. A Responsible Entity may choose to document one plan for communications between Control Centers it owns and a separate plan for communications between its Control Centers and the Control Centers of a neighboring Entity. The number and structure of the plans is at the discretion of the Responsible Entity as long as the plan(s) include the required elements described in parts 1.1, 1.2, and 1.3 of Requirement R1.

Identification of Security Protection

Entities have latitude to identify and choose which security protection is used to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers.

This security protection could consist of logical protection, physical protection, or some combination of both. To determine security protection, the requirement specifies that it must mitigate the risk of unauthorized disclosure or modification of applicable data.

Security protection implementation can be demonstrated in many ways. If a Responsible Entity uses physical protection, it may demonstrate implementation through review of an applicable Control Center floor plan with details subsequently confirmed through visual inspection, which identifies the physical security measures in place protecting the communication link. If the Responsible Entity uses logical protection, it may demonstrate implementation through an export of the device configuration which applies the security protection. Alternatively, a Responsible Entity may demonstrate implementation through security control monitoring, using an automated monitoring tool to generate reports on the encryption service used to protect a communications link. Where the operational obligations of an entire communication link, including both endpoints, belong to the Control Center of another Responsible Entity, the Responsible Entity without operational obligations for the communication link may demonstrate compliance by ensuring the communications link endpoint is within its Control Center, which could be limited to including the communication link endpoint within a PSP.

Identification of Where Security Protection is Applied by the Responsible Entity

A Responsible Entity should consider its environment when identifying where security protections should be applied. One approach is to implement security within the Control Center itself to ensure that data confidentiality and integrity is protected throughout the transmission. The Responsible Entity can identify where security protection is applied using a logical or physical location The application of security in accordance with CIP-012 requirements does not add additional assets to the scope of the CIP Reliability Standards. Locations of applied security protection may vary based on many factors such as impact levels of the Control Center, different technologies, or infrastructures. Where the operational obligations of an entire communication link, including both endpoints, belong to the Control Center of another Responsible Entity, the Responsible Entity without operational obligations for the communication link may demonstrate compliance by ensuring the communications link endpoint is within its Control Center, which could be limited to including the communication link endpoint within a PSP.

Identification of where a Responsible Entity applies security protection could be demonstrated with a list or a Control Center diagram showing either physical or logical security controls. Physical diagrams may require visual

confirmation of these controls. These diagrams or a list could be included within the plan developed for R1. A Responsible Entity could also use labels to identify on-site devices where CIP-012 security protection is applied.

When exchanging data between two entities, if a Responsible Entity only manages one end of a communication link, the Responsible Entity is not responsible for identifying where the security protection is applied by the neighboring entity with which it is exchanging data. However, if a Responsible Entity has taken responsibility for both ends of the communication link (such as by placing a router within the neighboring entity's data center), then the Responsible Entity shall identify where the security protection is applied at both ends of the link.

Similarly, if a Responsible Entity owns and operates both Control Centers which are exchanging data (such as in the case of a primary and backup Control Center), then the Responsible Entity shall identify where security protection is applied at both ends of the link.

Identification of Responsibilities when the Control Centers are Owned or Operated by Different Responsible Entities

The Technical Rationale and Justification for CIP-012-1 identifies key considerations in the Control Center Ownership section when communications between Control Centers with different owners or operators. Many operational relationships between Responsible Entities are unique. Consequently, there is no single way to identify responsibilities for applying security protection to the transmission of Real-time Assessment and Real-time monitoring data between Control Centers.

Implementation of responsibilities could also be demonstrated in many ways. Some examples include a joint procedure, a memorandum of understanding, or meeting minutes between the two parties where responsibilities are defined.

Where the operational obligations of an entire communication link, including both endpoints, belong to the Control Center of another Responsible Entity, the Responsible Entity without operational obligations for the communication link may demonstrate compliance by ensuring the communications link endpoint is within its Control Center, which could be limited to including the communication link endpoint within a PSP. These responsibilities should be included in both Responsible Entities' plans satisfying requirement part 1.3.

Reference Model

For this Implementation Guidance, the SDT uses a basic reference model of Primary and Backup Control Centers (Entity Alpha) to illustrate approaches to demonstrating compliance. These Control Centers communicate to each other and to a neighboring entity's Control Center (Entity Beta) in configurations outlined by the diagrams in this section. The SDT recognizes that the reference model does not contain many of the complexities of a real Control Center. For this Implementation Guidance, the registration or functions performed in the reference model Control Center are also not considered. A high level block diagram of the basic reference model is shown below in Figure 1. This Implementation Guidance is developed from the perspective of Entity Alpha.

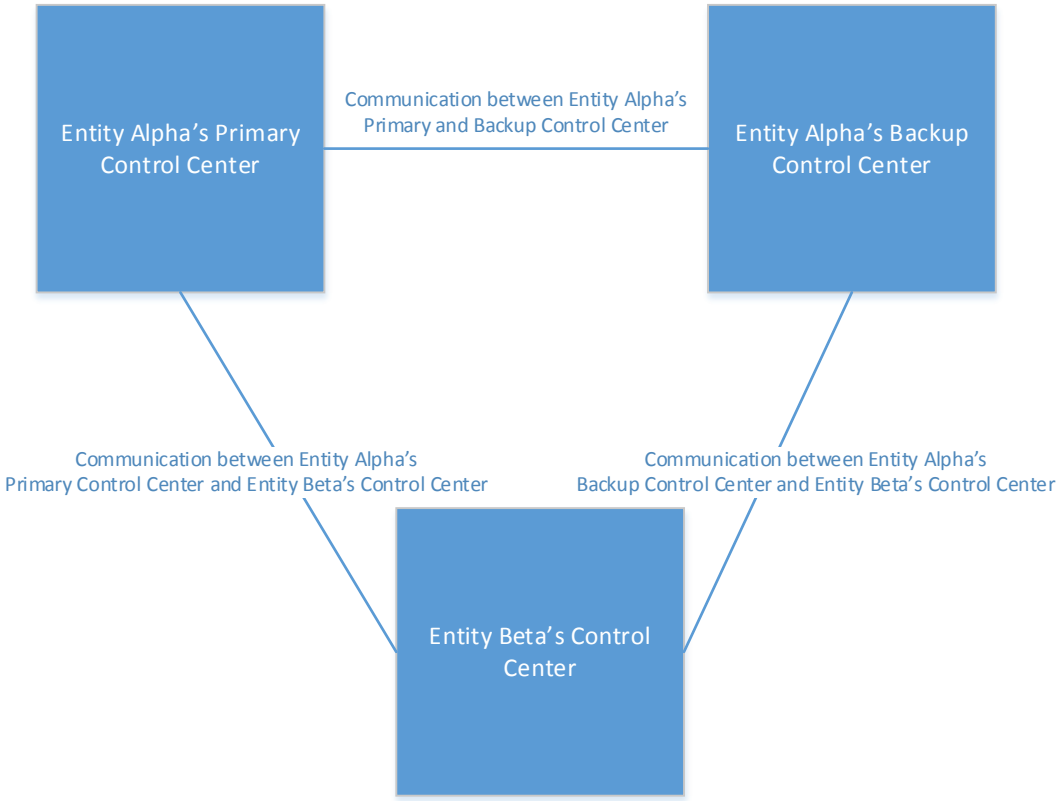


Figure 1: High Level Block Diagram of Reference Model Control Centers

Reference Model Discussion

Requirement R1 requires the implementation of a documented plan. To comply with requirement R1, one approach to a plan is to first determine which communications are in scope of CIP-012-1. There are multiple ways to identify an entity's scope in R1. For example, Entity Alpha in the reference model may first identify the Control Centers with which it communicates. Entity Alpha would determine that there are three: Entity Alpha's Primary Control Center, Entity Alpha's Backup Control Center, and Entity Beta's Control Center. Entity Alpha does not need to consider whether Entity Beta further shares its data with another Entity. That is the responsibility of Entity Beta and is outside of Entity Alpha's purview. Additionally, Entity Alpha does not need to consider any communications to other non-Control Center facilities such as generating plants or substations. These communications are out of scope for CIP-012-1.

Now that Entity Alpha has identified the Control Centers with which it communicates, Entity Alpha identifies either: (1) the Real-time Assessment and Real-time monitoring data; or (2) communication links which are used to transmit Real-time Assessment and Real-time monitoring data between Control Centers. In either case, Entity Alpha should refer to the data specification for Real-time Assessment and Real-time monitoring data identified in

TOP-003-3 and IRO-010-2. For this reference model scenario, identifying the communication links used to transmit Real-time Assessment and Real-time monitoring data may be the most straightforward approach. Through an evaluation of communication links between Control Centers and an evaluation of how it transmits and receives Real-time Assessment and Real-time monitoring data, Entity Alpha determined that it communicates applicable data between its primary and backup Control Centers across a single communication link. Entity Alpha also determined that it communicates applicable data to and from Entity Beta's Control Center across one of two links that originate from either Entity Alpha's primary or backup Control Center using the Inter-Control Center Communications Protocol (ICCP).

With an identified scope of communications links, Entity Alpha now considers the three required elements of its required communications between Control Centers for its plan.

Identification of Security Protection

- Entity Alpha must ensure that protection is applied where identified in its CIP-012-1 plan. The protection must also meet the security objective of mitigating the risk of unauthorized disclosure or modification of applicable data while in transit between Control Centers. The identification of security protection could be demonstrated by a network diagram similar to that shown in Figure 2 or Figure 3.
- In a simple case where the security protection is applied sufficiently close to the Control Center, such as within the Physical Security Perimeter of the Control Center, Entity Alpha may use a single security protection method to meet the security objective. For this case, shown in Figure 2, Entity Alpha implements a Virtual Private Network (VPN) connection across a private leased communication circuit for each of its three in-scope communication links. To meet the security objective, Entity Alpha further states that its VPN uses Internet Protocol security (IPsec) with encryption.
- For more complex scenarios, Entity Alpha may need to use a combination of security controls. For instance, in Figure 3, Entity Alpha uses a combination of physical security controls (physical access control) and logical security controls (encrypted communications consistent with the first scenario above) to meet the security objective. The SDT notes that the same technical architecture could exist where the responsibilities of the registered entities are different. Therefore as shown in Figure 2 & 3, in the scenario where entity Alpha owns and operationally manages the communication link and endpoint equipment, Entity Beta is responsible for ensuring the communication endpoint of the communication link is within a Control Center. Entity Beta ensures Entity Alpha's communication link endpoint equipment is within a Control Center by including the communication endpoint within a Control Center PSP. The physical controls for the PSP are described in CIP-006 documentation and do not need to be repeated for this requirement. This satisfies Entity Beta's obligation for Part 1.1 and 1.2.
- While these scenarios are all specific to communication links, it is possible that Entity Alpha and Entity Beta achieve the security objective by applying protection to the data rather than the communication links. In this scenario, the application enabling the data exchange between Control Centers may be capable of applying security controls directly to the data. These security controls mitigate the risk of unauthorized disclosure or modification of applicable data rather than relying on lower level network services to provide this security. For instance, Entity Alpha and Entity Beta may apply security protection at the application layer by using Secure ICCP to exchange applicable data. According to a report released by Sandia National Labs[2], Secure ICCP provides "data integrity indirectly by providing a cryptographic checksum. Secure ICCP provides data confidentiality by encrypting ICCP data exchanges." Methods other than Secure ICCP could also be used to apply security protection to the data at the application layer.
- It is theoretically possible that Entity Alpha and Entity Beta could exchange Real-time Assessment data between Control Centers by email. In that scenario, one approach may be for Entity Alpha to email the

[2] https://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/19-Secure_ICCP_Integration.pdf

applicable data to Entity Beta's Control Center in a protected container such as an encrypted zip file. Entity Alpha and Entity Beta can then exchange the password to that encrypted container through another method, such as by phone. While the notional example of protecting data exchanged by email is a useful illustration of how to achieve the security objective of CIP-012-1, it is extremely unlikely to be used in practice. The characteristics of email communication are inconsistent with the requirements of Real-time data exchange.

Identification of Where Security Protection is Applied by the Responsible Entity

Similar to the identification of security protection above, the identification of where security protection is applied can also be demonstrated by a network diagram similar to those found in Figures 2 and 3.

- Figure 2 shows the identification where CIP-012-1 security protection is applied for the Entity Alpha reference model when a single encrypted tunnel is used to implement the required protection. Entity Alpha has identified that security protection is applied at each of its Control Centers on the external Ethernet interface on the WAN router. While the diagram depicts where Entity Beta has applied security protection for illustrative purposes, Entity Alpha is not responsible for identifying where Entity Beta has applied security protection.
- In order to understand the application of security protection in context of who controls the communication link, it may be helpful to identify both where CIP-012-1 security protection is applied and the location of the telecommunications carrier (telco) demarcation point. Figure 3 provides such an example where the telco demarcation point may not be within the Control Center and based the facts and circumstances surrounding this scenario, Entity Alpha has implemented a combination of security controls to comply with CIP-012-1. In this scenario, Entity Alpha identifies that it has applied physical security protection for its PSP and continuing for its WAN router and that it has applied logical security protection (encryption) at the WAN router. Entity Alpha has also identified the telco demarcation point at a point in the telecommunications cabling connecting to Entity Alpha's WAN router, perhaps at a punch down block for example. In Figure 3, the telco demarcation point is inside the same room as the WAN router. The telco demarcation points are referenced in the drawing for clarity, but are not part of the plan.
- Figure 2 & 3 provides an example of where the operational obligations of an entire communications link, including both endpoints, belong to Entity Alpha. In this case, Entity Beta may be responsible for ensuring the communications endpoint of the communications link is within their Control Center. Entity Beta ensures Entity Alpha's communication link endpoint equipment is within a Control Center by including the communication endpoint within a Control Center PSP. The documentation provided for Part 1.1 by Entity Beta fulfils this obligation.
- The data-centric scenario described above is less intuitive for identifying where security protection is applied by Entity Alpha. If security protection is applied at the application layer (such as Secure ICCP), Entity Alpha could reasonably identify the application or service applying the security (such as the Secure ICCP service) as the location of where security protection is applied.

Identification of Responsibilities when the Control Centers are Owned or Operated by Different Responsible Entities

Entity Alpha and Entity Beta may determine they each are responsible for one end of the VPN configuration on their respective WAN routers. Entity Alpha and Entity Beta have agreed to a 30 character pre-shared key for IPSec authentication.

Rather than use a pre-shared key, Entity Alpha and Entity Beta may decide to use digital certificates for the IPSec authentication using a trusted certificate authority. In that scenario, Entity Alpha and Entity Beta would agree on who is the party responsible for managing the certificate authority.

In the example where the communication link and endpoint equipment are owned by Entity Alpha, both entities should include ownership responsibilities in their plans satisfying requirement 1.3. Examples include but are not

limited to, a letter indicating ownership or responsibility, a copy of a contract indicating ownership or responsibilities, an excerpt from an operational agreement or manual indicating ownership or responsibility.

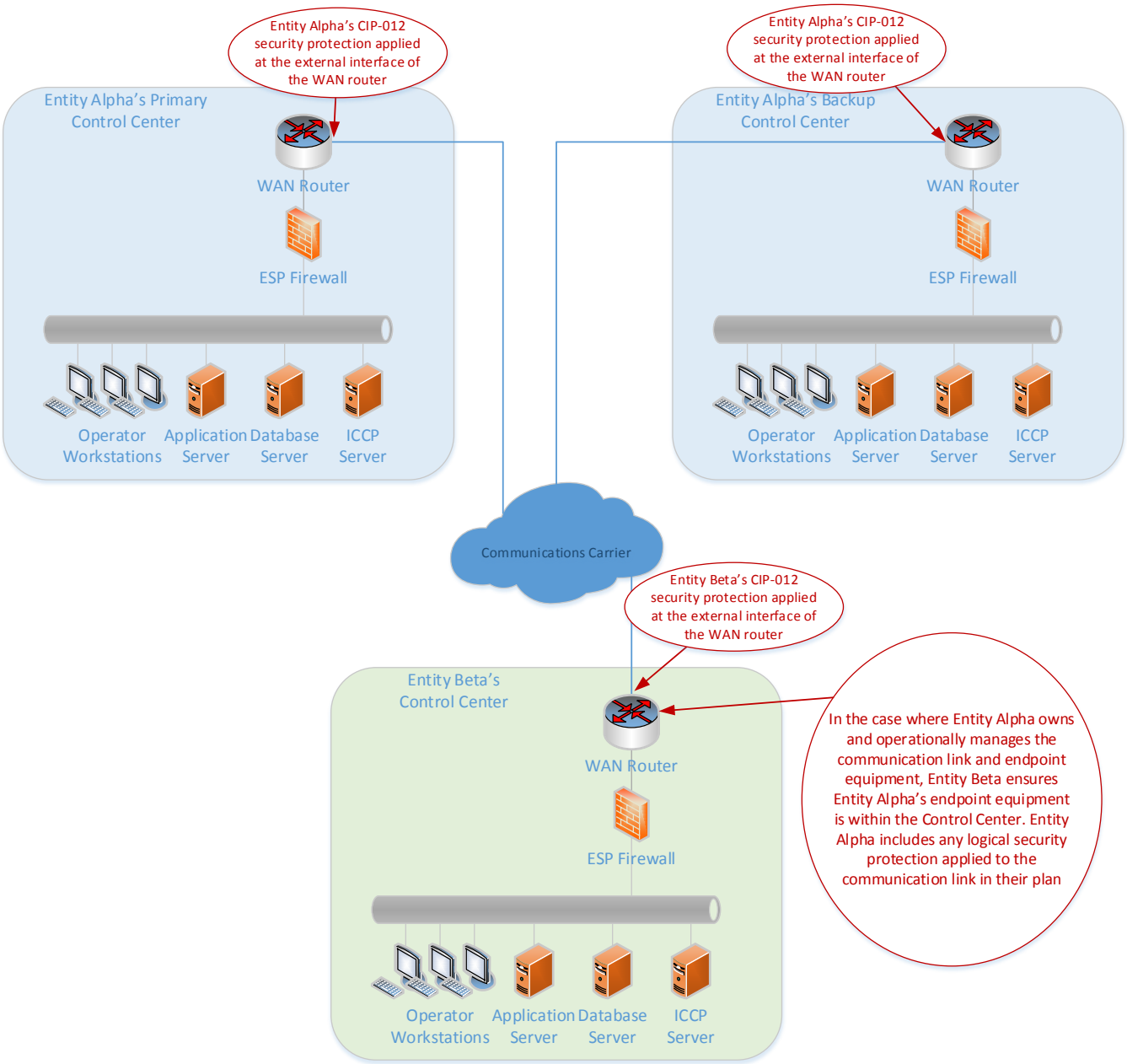


Figure 2: Network diagram and identification of where security protection is applied

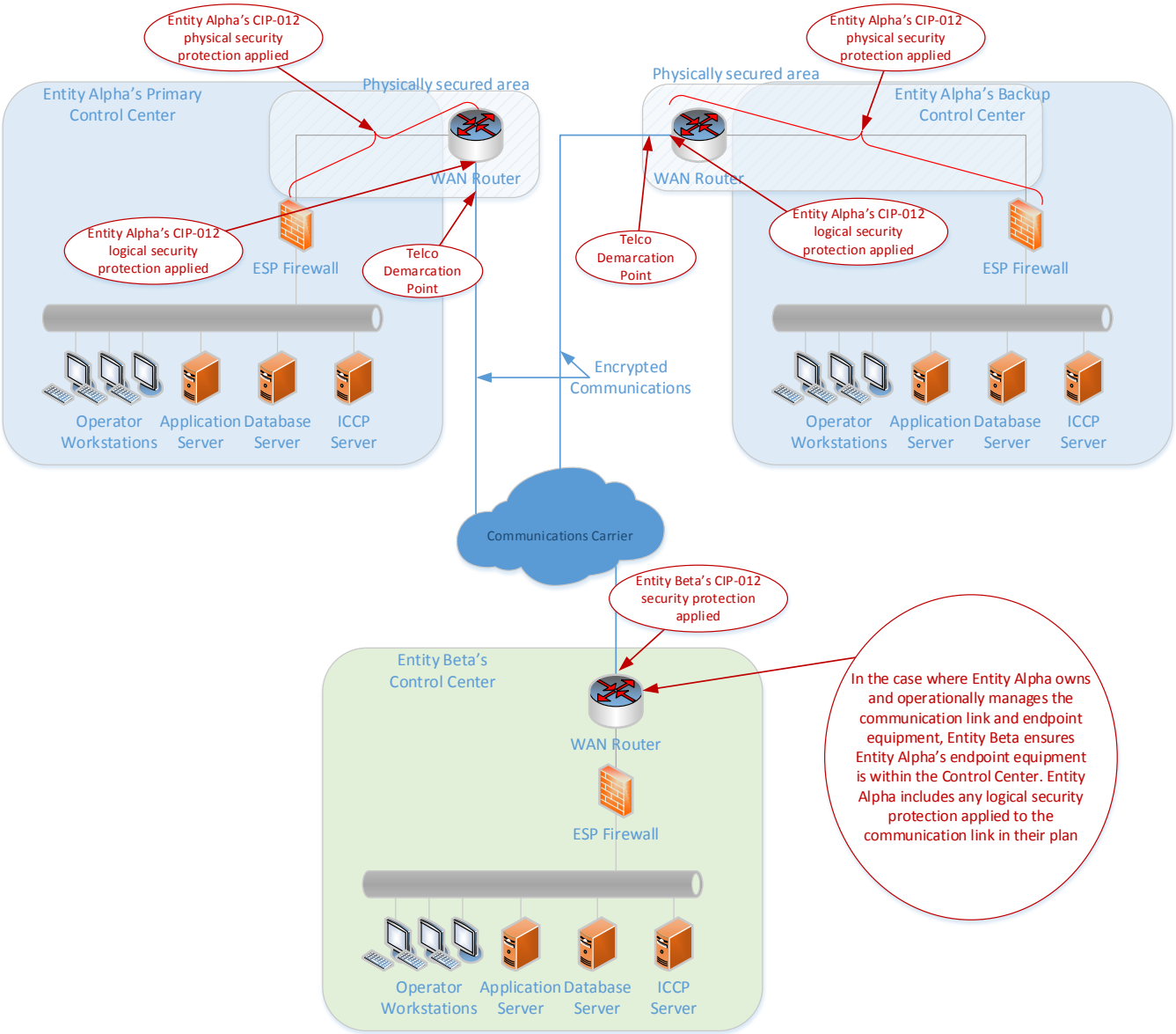


Figure 3: Network diagram using a combination of controls for CIP-012-1

References

Mitre Common Weakness Enumeration (CWE™) list of software weakness types
https://cwe.mitre.org/data/definitions/327.html

Cryptographic Standards and Guidelines
https://csrc.nist.gov/Projects/Cryptographic-Standards-and-Guidelines

NIST Special Publication 800-175B
Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-175B.pdf

Guide to Cryptography
https://www.owasp.org/index.php/Guide_to_Cryptography#Symmetric_Cryptography

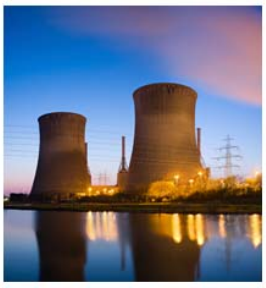
NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DRAFT

Cyber Security – Communications Between Control Centers

Implementation Guidance for CIP-012-1

RELIABILITY | ACCOUNTABILITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Introduction

The Project 2016-02 SDT drafted this Implementation Guidance to provide example approaches for compliance with CIP-012-1. Implementation Guidance does not prescribe the only approach, but highlights one or more approaches that would be effective in achieving compliance with the standard. Because Implementation Guidance only provides examples, entities may choose alternative approaches that better fit their individual situations[1].

Responsible Entities may find it useful to consider this Implementation Guidance document along with the additional context and background provided in the SDT-developed Technical Rationale and Justification for CIP-012-1 document.

Background

The Commission issued Order No. 822 on January 21, 2016. Order 822 ~~approving seven~~approving seven CIP Reliability Standards and new or modified definitions, and directed modifications be made to the CIP Reliability Standards. Among other items, the Commission directed NERC to "develop modifications to the CIP Reliability Standards to require responsible entities to implement controls to protect, at a minimum, communication links and sensitive bulk electric system data communicated between bulk electric system Control Centers in a manner that is appropriately tailored to address the risks posed to the bulk electric system by the assets being protected (i.e., high, medium, or low impact)." (Order 822, Paragraph 53)

In response to the directive in Order No. 822, the Project 2016-02 standard drafting team (SDT) drafted Reliability Standard CIP-012-1 to require Responsible Entities to implement controls to protect sensitive Bulk Electric System (BES) data and communications links between BES Control Centers. Due to the sensitivity of the data being communicated between Control Centers, the standard applies to all impact levels (i.e., high, medium, or low impact).

The SDT drafted requirements to provide Responsible Entities the latitude to protect the communication links, the data, or both, to satisfy the security objective consistent with the capabilities of the Responsible Entity's operational environment.

[1] NERC's Compliance Guidance Policy

Requirements

R1. *The Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring data while being transmitted between any applicable Control Centers. ~~This requirement excludes oral communications~~The Responsible Entity is not required to include oral communications in its plan. The plan shall include: [Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. Identification of security protection used to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers;

1.2. Identification of where the Responsible Entity applied security protection for transmitting Real-time Assessment and Real-time monitoring and control data between Control Centers; and

1.3. If the Control Centers are owned or operated by different Responsible Entities, identify the responsibilities of each Responsible Entity for applying security protection to the transmission of Real-time Assessment and Real-time monitoring data between those Control Centers.

General Considerations

Plan Development

As noted in the Technical Rationale and Justification for CIP-012-1, the focus of Requirement R1 is ~~-~~implementing a documented plan to protect information that is critical to the real-time operations of the Bulk Electric System while in transit between applicable Control Centers. The number of plan(s) and their content may vary depending on a Responsible Entity's management structure and operating conditions. The Responsible Entity may document as many plans as necessary to meet its needs. For instance, a Responsible Entity may choose to document one plan per Control Center or choose an all-inclusive, single plan for its Control Center communication environment. A Responsible Entity may choose to document one plan for communications between Control Centers it owns and a separate plan for communications between its Control Centers and the Control Centers of a neighboring Entity. The number and structure of the plans is at the discretion of the Responsible Entity as long as the plan(s) include the required elements described in parts 1.1, 1.2, and 1.3 of Requirement R1.

Identification of Security Protection

Entities have latitude to identify and choose which security protection is used to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers.

This security protection could consist of logical protection, physical protection, or some combination of both. To determine security protection, the requirement specifies that it must mitigate the risk of unauthorized disclosure or modification of applicable data.

Security protection implementation can be demonstrated in many ways. If a Responsible Entity uses physical protection, it may demonstrate implementation through review of an applicable Control Center floor plan with details subsequently confirmed through visual inspection, which identifies the physical security measures in place protecting the communication link. If the Responsible Entity uses logical protection, it may demonstrate implementation through an export of the device configuration which applies the security protection. Alternatively, a Responsible Entity may demonstrate implementation through security control monitoring, using an automated monitoring tool to generate reports on the encryption service used to protect a communications link. Where the operational obligations of an entire communication link, including both endpoints, belong to the Control Center of another Responsible Entity, the Responsible Entity without operational obligations for the communication link may demonstrate compliance by ensuring the communications link endpoint is within its Control Center, which could be limited to including the communication link endpoint within a PSP.

Identification of ~~-~~Where Security Protection is Applied by the Responsible Entity

A Responsible Entity should consider its environment when identifying where security protections should be applied. One approach is to implement security within the Control Center itself to ensure that data confidentiality and integrity is protected throughout the transmission. The Responsible Entity can identify where security protection is applied using a logical or physical location The application of security in accordance with CIP-012 requirements does not add additional assets to the scope of the CIP Reliability Standards. Locations of applied security protection may vary based on many factors such as impact levels of the Control Center, different technologies, or infrastructures. Where the operational obligations of an entire communication link, including both endpoints, belong to the Control Center of another Responsible Entity, the Responsible Entity without operational obligations for the communication link may demonstrate compliance by ensuring the communications link endpoint is within its Control Center, which could be limited to including the communication link endpoint within a PSP.

Identification of where a Responsible Entity applies security protection could be demonstrated with a list or a Control Center diagram showing either physical or logical security controls. Physical diagrams may require visual

confirmation of these controls. These diagrams or a list could be included within the plan developed for R1. A Responsible Entity could also use labels to identify on-site devices where CIP-012 security protection is applied.

When exchanging data between two entities, if a Responsible Entity only manages one end of a communication link, the Responsible Entity is not responsible for identifying where the security protection is applied by the neighboring entity with ~~whom~~which it is exchanging data. ~~–~~However, if a Responsible Entity has taken responsibility for both ends of the communication link (such as by placing a router within the neighboring entity's data center), then the Responsible Entity shall identify where the security protection is applied at both ends of the link.

Similarly, if a Responsible Entity owns and operates both Control Centers which are exchanging data (such as in the case of a primary and backup Control Center), then the Responsible Entity shall identify where security protection is applied at both ends of the link.

Identification of Responsibilities when the Control Centers are Owned or Operated by Different Responsible Entities

The Technical Rationale and Justification for CIP-012-1 identifies key considerations in the Control Center Ownership section when communications between Control Centers with different owners or operators. Many operational relationships between Responsible Entities are unique. Consequently, there is no single way to identify responsibilities for applying security protection to the transmission of Real-time Assessment and Real-time monitoring data between Control Centers.

Implementation of responsibilities could also be demonstrated in many ways. Some examples include a joint procedure, a memorandum of understanding, or meeting minutes between the two parties where responsibilities are defined.

Where the operational obligations of an entire communication link, including both endpoints, belong to the Control Center of another Responsible Entity, the Responsible Entity without operational obligations for the communication link may demonstrate compliance by ensuring the communications link endpoint is within its Control Center, which could be limited to including the communication link endpoint within a PSP. ~~–~~These responsibilities should be included in both Responsible Entities' plans satisfying requirement part 1.3.

Reference Model

For this Implementation Guidance, the SDT uses a basic reference model of Primary and Backup Control Centers (Entity Alpha) to illustrate approaches to demonstrating compliance. These Control Centers communicate to each other and to a neighboring entity's Control Center (Entity Beta) in configurations outlined by the diagrams in this section. The SDT recognizes that the reference model does not contain many of the complexities of a real Control Center. For this Implementation Guidance, the registration or functions performed in the reference model Control Center are also not considered. A high level block diagram of the basic reference model is shown below in Figure 1. -This Implementation Guidance is developed from the perspective of Entity Alpha.

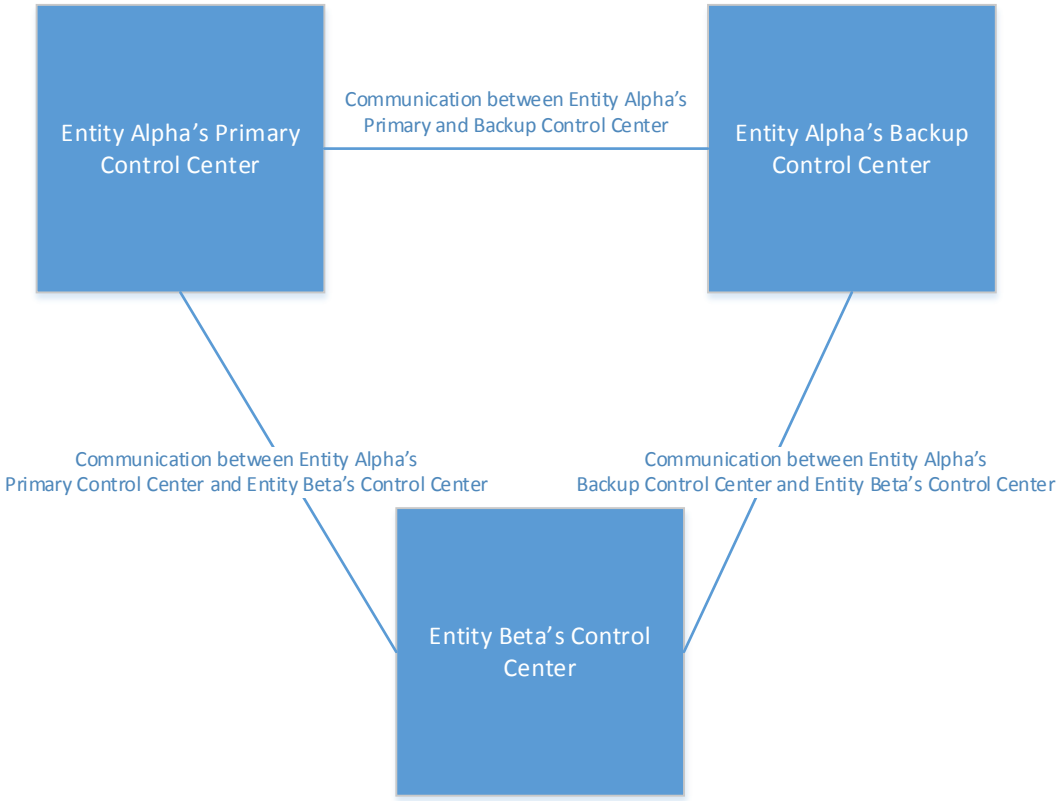


Figure 1: High Level Block Diagram of Reference Model Control Centers

Reference Model Discussion

Requirement R1 requires the implementation of a documented plan. To comply with requirement R1, one approach to a plan is to first determine which communications are in scope of CIP-012-1. There are multiple ways to identify an entity's scope in R1. For example, Entity Alpha in the reference model may first identify the Control Centers with which it communicates. Entity Alpha would determine that there are three: Entity Alpha's Primary Control Center, Entity Alpha's Backup Control Center, and Entity Beta's Control Center.– Entity Alpha does not need to consider whether Entity Beta further shares its data with another Entity. That is the responsibility of Entity Beta and is outside of Entity Alpha's purview. Additionally, Entity Alpha does not need to consider any communications to other non-Control Center facilities such as generating plants or substations. –These communications are out of scope for CIP-012-1.

Now that Entity Alpha has identified the Control Centers with which it communicates, Entity Alpha identifies either: (1) the Real-time Assessment and Real-time monitoring data; or (2) communication links which are used to transmit Real-time Assessment and Real-time monitoring data between Control Centers. In either case, Entity Alpha should refer to the data specification for Real-time Assessment and Real-time monitoring data identified in

TOP-003-3 and IRO-010-2. For this reference model scenario, identifying the communication links used to transmit Real-time Assessment and Real-time monitoring data may be the most straightforward approach. Through an evaluation of communication links between Control Centers and an evaluation of how it transmits and receives Real-time Assessment and Real-time monitoring data, Entity Alpha determined that it communicates applicable data between its primary and backup Control Centers across a single communication link. Entity Alpha also determined that it communicates applicable data to and from Entity Beta's Control Center across one of two links that originate from either Entity Alpha's primary or backup Control Center using the Inter-Control Center Communications Protocol (ICCP).

With an identified scope of communications links, Entity Alpha now considers the three required elements of its required communications between Control Centers for its plan.

Identification of Security Protection

- Entity Alpha must ensure that protection is applied where identified in its CIP-012-1 plan. The protection must also meet the security objective of mitigating the risk of unauthorized disclosure or modification of applicable data while in transit between Control Centers. The identification of security protection could be demonstrated by a network diagram similar to that shown in Figure 2 or Figure 3.
- In a simple case where the security protection is applied sufficiently close to the Control Center, such as within the Physical Security Perimeter of the Control Center, Entity Alpha may use a single security protection method to meet the security objective. For this case, shown in Figure 2, Entity Alpha implements a Virtual Private Network (VPN) connection across a private leased communication circuit for each of its three in-scope communication links. To meet the security objective, Entity Alpha further states that its VPN uses Internet Protocol security (IPsec) with encryption.
- For more complex scenarios, Entity Alpha may need to use a combination of security controls. ~~–~~For instance, in Figure 3, Entity Alpha uses a combination of physical security controls (physical access control) and logical security controls (encrypted communications consistent with the first scenario above) to meet the security objective.~~–~~ The SDT notes that the same technical architecture could exist where the responsibilities of the registered entities are different. ~~Alternately~~Therefore as shown in Figure 2 & 3, in the scenario where entity Alpha owns and operationally manages the communication link and endpoint equipment, Entity Beta is responsible for ensuring the communication endpoint of the communication link is within a Control Center. Entity Beta ensures Entity Alpha's communication link endpoint equipment is within a Control Center by including the communication endpoint within a Control Center PSP. ~~–~~The physical controls for the PSP are described in CIP-006 documentation and do not need to be repeated for this requirement. This satisfies Entity Beta's obligation for Part 1.1 and 1.2.
- While these scenarios are all specific to communication links, it is possible that Entity Alpha and Entity Beta achieve the security objective by applying protection to the data rather than the communication links. In this scenario, the application enabling the data exchange between Control Centers may be capable of applying security controls directly to the data. These security controls mitigate the risk of unauthorized disclosure or modification of applicable data rather than relying on lower level network services to provide this security. For instance, Entity Alpha and Entity Beta may apply security protection at the application layer by using Secure ICCP to exchange applicable data. According to a report released by Sandia National Labs[2], Secure ICCP provides "data integrity indirectly by providing a cryptographic checksum. Secure ICCP provides data confidentiality by encrypting ICCP data exchanges." Methods other than Secure ICCP could also be used to apply security protection to the data at the application layer.
- It is theoretically possible that Entity Alpha and Entity Beta could exchange Real-time Assessment data between Control Centers by email. In that scenario, one approach may be for Entity Alpha to email the

[2] https://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/19-Secure_ICCP_Integration.pdf

applicable data to Entity Beta's Control Center in a protected container such as an encrypted zip file. Entity Alpha and Entity Beta can then exchange the password to that encrypted container through another method, such as by phone. While the notional example of protecting data exchanged by email is a useful illustration of how to achieve the security objective of CIP-012-1, it is extremely unlikely to be used in practice. The characteristics of email communication are inconsistent with the requirements of Real-time data exchange.

Identification of Where Security Protection is Applied by the Responsible Entity

Similar to the identification of security protection above, the identification of where security protection is applied can also be demonstrated by a network diagram similar to those found in Figures 2 and 3.

- Figure 2 shows the identification where CIP-012-1 security protection is applied for the Entity Alpha reference model when a single encrypted tunnel is used to implement the required protection. Entity Alpha has identified that security protection is applied at each of its Control Centers on the external Ethernet interface on the WAN router. While the diagram depicts where Entity Beta has applied security protection for illustrative purposes, Entity Alpha is not responsible for identifying where Entity Beta has applied security protection.

- In order to understand the application of security protection in context of who controls the communication link, it may be helpful to identify both where CIP-012-1 security protection is applied and the location of the telecommunications carrier (telco) demarcation point. Figure 3 provides such an example where the telco demarcation point may not be within the Control Center and based the facts and ~~circumstances surrounding this scenario, Entity Alpha has~~circumstances~~'~~ surrounding this scenario, Entity Alpha has implemented a combination of security controls to comply with CIP-012-1. In this scenario, Entity Alpha identifies that it has applied physical security protection for its PSP and continuing for its WAN router and that it has applied logical security protection (encryption) at the WAN router. Entity Alpha has also identified the telco demarcation point at a point in the telecommunications cabling connecting to Entity Alpha's WAN router, perhaps at a punch down block for example. In Figure 3, the telco demarcation point is inside the same room as the WAN router. The telco demarcation points are referenced in the drawing for clarity, but are not part of the plan.

- Figure 2 & 3 provides an example of where the operational obligations of an entire communications link, including both endpoints, belong to Entity Alpha. -In this case, Entity Beta may be responsible for ensuring the communications endpoint of the communications link is within their Control Center. Entity Beta ensures Entity Alpha's communication link endpoint equipment is within a Control Center by including the communication endpoint within a Control Center PSP. The documentation provided for Part 1.1 by Entity Beta fulfils this obligation.

- The data-centric scenario described above is less intuitive for identifying where security protection is applied by Entity Alpha. If security protection is applied at the application layer (such as Secure ICCP), Entity Alpha could reasonably identify the application or service applying the security (such as the Secure ICCP service) as the location of where security protection is applied.

Identification of Responsibilities when the Control Centers are Owned or Operated by Different Responsible Entities

Entity Alpha and Entity Beta may determine they each are responsible for one end of the VPN configuration on their respective WAN routers. Entity Alpha and Entity Beta have agreed to a 30 character pre-shared key for IPSec authentication.

Rather than use a pre-shared key, Entity Alpha and Entity Beta may decide to use digital certificates for the IPSec authentication using a trusted certificate authority. In that scenario, Entity Alpha and Entity Beta would agree on who is the party responsible for managing the certificate authority.

In the example where the communication link and endpoint equipment are owned by Entity Alpha, both entities should include ownership responsibilities in their plans satisfying requirement 1.3. Examples include but are not limited to, a letter ~~stating~~ indicating ownership or responsibility, a copy of a contract indicating ownership or responsibilities, an excerpt from an operational agreement or manual indicating ownership or responsibility.

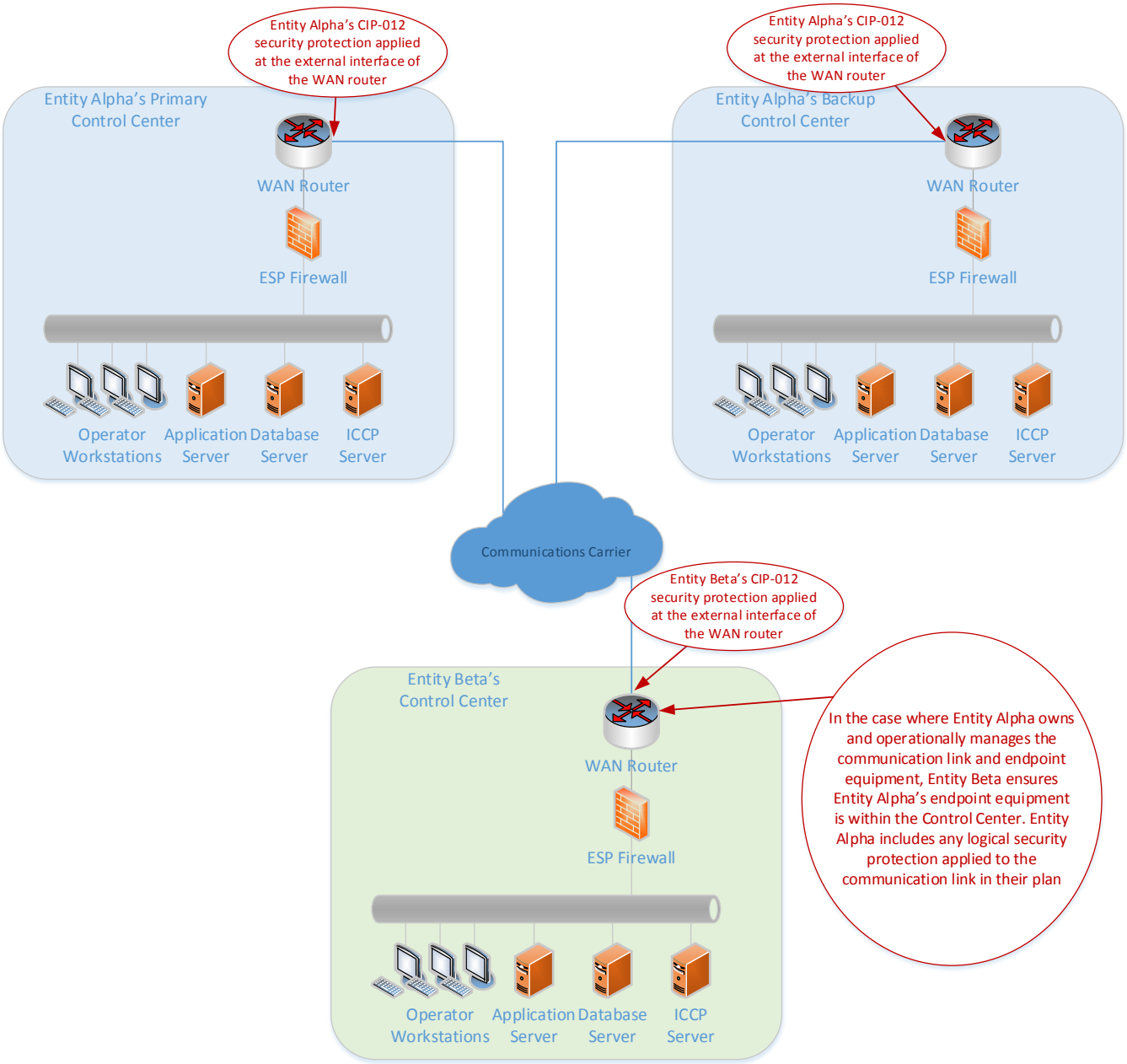


Figure 2: Network diagram and identification of where security protection is applied

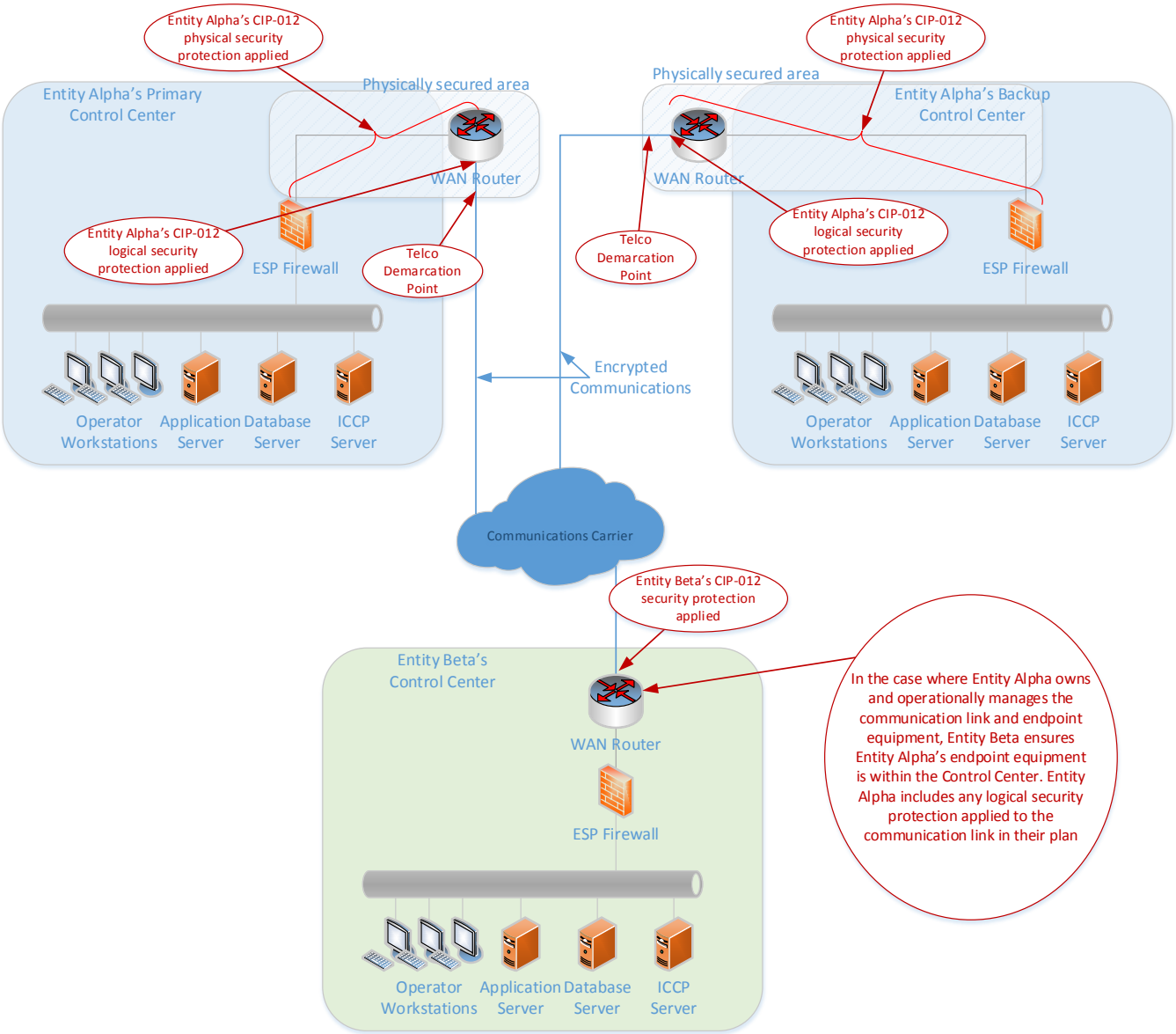


Figure 3: Network diagram using a combination of controls for CIP-012-1

References

Mitre Common Weakness Enumeration (CWE™) list of software weakness types
https://cwe.mitre.org/data/definitions/327.html

Cryptographic Standards and Guidelines
https://csrc.nist.gov/Projects/Cryptographic-Standards-and-Guidelines

NIST Special Publication 800-175B
Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-175B.pdf

Guide to Cryptography
https://www.owasp.org/index.php/Guide_to_Cryptography#Symmetric_Cryptography

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Reliability Standard Audit Worksheet[1]

CIP-012-1 – Cyber Security – Communications between Control Centers

This section to be completed by the Compliance Enforcement Authority.

Audit ID:	Audit ID if available; or REG-NCRnnnnn-YYYYMMDD
Registered Entity:	Registered name of entity being audited
NCR Number:	NCRnnnnn
Compliance Enforcement Authority:	Region or NERC performing audit
Compliance Assessment Date(s)[2]:	Month DD, YYYY, to Month DD, YYYY
Compliance Monitoring Method:	[On-site Audit | Off-site Audit | Spot Check]
Names of Auditors:	Supplied by CEA

Applicability of Requirements

	BA	DP	GO	GOP	PA/PC	RC	RP	RSG	TO	TOP	TP	TSP
R1	X		X	X		X			X	X		

Legend:

Text with blue background:	Fixed text – do not edit
Text entry area with Green background:	Entity-supplied information
Text entry area with white background:	Auditor-supplied information

[1] NERC developed this Reliability Standard Audit Worksheet (RSAW) language in order to facilitate NERC's and the Regional Entities' assessment of a registered entity's compliance with this Reliability Standard. The NERC RSAW language is written to specific versions of each NERC Reliability Standard. Entities using this RSAW should choose the version of the RSAW applicable to the Reliability Standard being assessed. While the information included in this RSAW provides some of the methodology that NERC has elected to use to assess compliance with the requirements of the Reliability Standard, this document should not be treated as a substitute for the Reliability Standard or viewed as additional Reliability Standard requirements. In all cases, the Regional Entity should rely on the language contained in the Reliability Standard itself, and not on the language contained in this RSAW, to determine compliance with the Reliability Standard. NERC's Reliability Standards can be found on NERC's website. Additionally, NERC Reliability Standards are updated frequently, and this RSAW may not necessarily be updated with the same frequency. Therefore, it is imperative that entities treat this RSAW as a reference document only, and not as a substitute or replacement for the Reliability Standard. It is the responsibility of the registered entity to verify its compliance with the latest approved version of the Reliability Standards, by the applicable governmental authority, relevant to its registration status.

The RSAW may provide a non-exclusive list, for informational purposes only, of examples of the types of evidence a registered entity may produce or may be asked to produce to demonstrate compliance with the Reliability Standard. A registered entity's adherence to the examples contained within this RSAW does not necessarily constitute compliance with the applicable Reliability Standard, and NERC and the Regional Entity using this RSAW reserve the right to request additional evidence from the registered entity that is not included in this RSAW. This RSAW may include excerpts from FERC Orders and other regulatory references which are provided for ease of reference only, and this document does not necessarily include all applicable Order provisions. In the event of a discrepancy between FERC Orders, and the language included in this document, FERC Orders shall prevail.

[2] Compliance Assessment Date(s): The date(s) the actual compliance assessment (on-site audit, off-site spot check, etc.) occurs.

Findings

(This section to be completed by the Compliance Enforcement Authority)

Req.	Finding	Summary and Documentation	Functions Monitored
R1			

Req.	Areas of Concern

Req.	Recommendations

Req.	Positive Observations

Subject Matter Experts

Identify the Subject Matter Expert(s) responsible for this Reliability Standard.

Registered Entity Response (Required; Insert additional rows if needed):

SME Name	Title	Organization	Requirement(s)

Registered Entity Response (Required):

Question 1: Does the Registered Entity own or operate an applicable Control Center? ☐ Yes ☐ No

If no:

1. Provide evidence in the space below that the Registered Entity does not own or operate an applicable Control Center. This evidence may include, but is not limited to:
   - Evidence that the Registered Entity does not own or operate an applicable Control Center; or
   - Evidence or a reference to evidence from the Registered Entity's CIP-002 compliance program that demonstrates the Registered Entity does not own or operate an applicable Control Center.
2. The remainder of this RSAW may be left blank.

[Note: A separate spreadsheet or other document may be used. If so, provide the document reference below.]

R1 Supporting Evidence and Documentation

R1. The Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring data while being transmitted between any applicable Control Centers. The Responsible Entity is not required to include oral communications in its plan. The plan shall include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1 Identification of security protection used to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers;

1.2 Identification of where the Responsible Entity applied security protection for transmitting Real-time Assessment and Real-time monitoring data between Control Centers; and

1.3 If the Control Centers are owned or operated by different Responsible Entities, identify the responsibilities of each Responsible Entity for applying security protection to the transmission of Real-time Assessment and Real-time monitoring data between those Control Centers.

M1. Evidence may include, but is not limited to, documented plan(s) that meet the security objective of Requirement R1 and documentation demonstrating the implementation of the plan(s).

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-012-1, R1

This section to be completed by the Compliance Enforcement Authority

	If the Registered Entity has answered "No" to Question 1, verify the Registered Entity does not own or operate an applicable Control Center. Note: If the Registered Entity does not own or operate an applicable Control Center, the remainder of this RSAW is not applicable.
	Verify the entity has implemented, except under CIP Exceptional Circumstances, one or more documented plan(s) to mitigate the risk of the unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring data while being transmitted between any applicable Control Centers.
	Verify the documented plans collectively include identification of security protection used to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring data while being transmitted between any applicable Control Centers.
	Verify the documented plans collectively include identification of where the Responsible Entity applied security protection for transmitting Real-time Assessment and Real-time monitoring data between any applicable Control Centers.
	If Real-time Assessment or Real-time monitoring data is transmitted between any applicable Control Centers owned or operated by different Responsible Entities, verify the documented plans collectively include identification of the responsibilities of each Responsible Entity for applying security protection to these transmissions.
	Verify the documented plans collectively achieve the security objective of mitigating the risk of the unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring data while being transmitted between any applicable Control Centers.
	If the Responsible Entity has declared and responded to CIP Exceptional Circumstances, verify the Responsible Entity has adhered to the applicable cyber security policies.
Notes to Auditor: 1. The Responsible Entity is not required to include oral communications in its plan. 2. See Applicability Section 4.2.3 for a decription of Control Centers that are exempt from this Standard.	

Auditor Notes:

Additional Information:

Reliability Standard

The full text of CIP-012-1 may be found on the NERC Web Site (www.nerc.com) under "Program Areas & Departments", "Standards," "Reliability Standards."

In addition to the Reliability Standard, there is an applicable Implementation Plan available on the NERC Web Site.

In addition to the Reliability Standard, there is background information available on the NERC Web Site.

Capitalized terms in the Reliability Standard refer to terms in the NERC Glossary, which may be found on the NERC Web Site.

Sampling Methodology

Sampling is essential for auditing compliance with NERC Reliability Standards since it is not always possible or practical to test 100% of either the equipment, documentation, or both, associated with the full suite of enforceable standards. The Sampling Guide contained in the Compliance Monitoring and Enforcement Manual (see NERC website) provided by the Electric Reliability Organization help to establish a minimum sample set for monitoring and enforcement uses in audits of NERC Reliability Standards.

Regulatory Language

FERC Order 822 P53-56, 58, and 62

Selected Glossary Terms

The following Glossary terms are provided for convenience only. Please refer to the NERC web site for the current enforceable terms.

CIP Exceptional Circumstance

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.

Control Center

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, of:

1) a Reliability Coordinator,
2) a Balancing Authority,
3) a Transmission Operator for transmission Facilities at two or more locations, or
4) a Generator Operator for generation Facilities at two or more locations.

Real-time Assessment

An evaluation of system conditions using Real-time data to assess existing (pre-Contingency) and potential (post-Contingency) operating conditions. The assessment shall reflect applicable inputs including, but not limited to: load, generation output levels, known Protection System and Special Protection System status or degradation, Transmission outages, generator outages, Interchange, Facility Ratings, and identified phase angle and equipment limitations. (Real-time Assessment may be provided through internal systems or through third-party services.)

Real-time

Present time as opposed to future time.

Revision History for RSAW

Version	Date	Reviewers	Revision Description
Draft1 v1	07/28/2017	NERC Stds Group	New document
Draft1 v2	08/01/2017	RSAW Task Force	Modified Question to clarify applicability
Draft1 v3	08/02/2017	RSAW Task Force	Response to MRO comments. Moved Questions 1 and 2 above R1. Made text changes to Q1 and to R2 Compliance Assessment Approach.
Draft1 v4	08/07/2017	RSAW Task Force, 2016-02 SDT	Response to TexasRE and SDT comments. Clarified scope of Q1 to be data transmitted between Control Centers. Removed extra space from Auditor Notes.
Draft2 v1	10/27/2017	RSAW Task Force	Modified title. Modified Q2 to conform with new language. Modified R1 with new Requirement text and new Compliance Assessment Approach. Modified R2 with new Compliance Assessment Approach. Removed Operational Planning Analysis from the Selected Glossary Terms. Modified footer with revised version and date.
Draft2 v2	11/27/2017	RSAW Task Force, Standard Drafting Team	Response to comments: • RF: Footnote 1 page 1 added space after “references.” • RF: Changed “Tasf” to “Task” in Revision History. • Response to SERC CIPC and Southern Company comments to Draft 1. • Modified Question 1 to include reference to CIP-002. • Added an item to the R1 Compliance Assessment Approach to verify the effectiveness of the process. • Modified the R2 Compliance Assessment Approaches to clarify that the review is for implementation.
Draft3 v0	03/20/2018	RSAW Task Force	Modified for Draft 3 language: • Removed Requirement R2 • Modified Requirement R1 language to match the Standard • Modified the R1 Compliannce Assessment Approach

			• Removed "CIP Exceptional Circumstance" from the Selected Glossary Terms • Revised the definition of "Control Center" in Selected Glossary Terms to match the definition posted alongside CIP-012-1 Draft 3
Draft3 v1	04/03/2018	ERO Enterprise	• Consideration of Comments from RF o Changed Sampling Methodology section to match current NERC documents. Will also need to be reflected in the RSAW Template.
Draft3 v2	4/25/2018	NERC Legal	Addressed comments. No text changes were made.
Draft4 v0	5/19/2018	RSAW Task Force	Modified for Draft 4 language: • Modified Question 1 to reference "applicable" Control Centers • Modified Requirement R1 language to match the Standard • Modified the R1 Compliance Assessment Approach • Modified the Note to Auditor in Compliance Assessment Approach • Restored the definition of "CIP Exceptional Circumstance" to the Selected Glossary Terms • Restored the approved definition of "Control Center" to the Selected Glossary Terms
Draft4 v1	6/4/2018	RSAW Task Force	Modified language of Question 1 to more closely match the Standard.
Draft4 v2	6/11/2018	NERC Compliance /NERC Legal	Addressed corrections/comments from NERC: • Corrected "entity" to "Registered Entity" in Question 1 • Addressed question regarding use of (s) in certain cases • Corrected "of responsibilities" to "of the responsibilities" in CAA item 5 • Addressed comment regarding CAA item 5 • Addressed comment regarding additional Note to Auditor • Removed underlining from definition of Control Center

			• Inserted hyphen into real-time in Control Center definition • Added “any applicable” Control Center to CAA items 3, 4, and 6.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Reliability Standard Audit Worksheet[1]

CIP-012-1 – Cyber Security – Communications between Control Centers

This section to be completed by the Compliance Enforcement Authority.

Audit ID:	Audit ID if available; or REG-NCRnnnnn-YYYYMMDD
Registered Entity:	Registered name of entity being audited
NCR Number:	NCRnnnnn
Compliance Enforcement Authority:	Region or NERC performing audit
Compliance Assessment Date(s)[2]:	Month DD, YYYY, to Month DD, YYYY
Compliance Monitoring Method:	[On-site Audit | Off-site Audit | Spot Check]
Names of Auditors:	Supplied by CEA

Applicability of Requirements

	BA	DP	GO	GOP	PA/PC	RC	RP	RSG	TO	TOP	TP	TSP
R1	X		X	X		X			X	X		

Legend:

Text with blue background:	Fixed text – do not edit
Text entry area with Green background:	Entity-supplied information
Text entry area with white background:	Auditor-supplied information

[1] NERC developed this Reliability Standard Audit Worksheet (RSAW) language in order to facilitate NERC's and the Regional Entities' assessment of a registered entity's compliance with this Reliability Standard. The NERC RSAW language is written to specific versions of each NERC Reliability Standard. Entities using this RSAW should choose the version of the RSAW applicable to the Reliability Standard being assessed. While the information included in this RSAW provides some of the methodology that NERC has elected to use to assess compliance with the requirements of the Reliability Standard, this document should not be treated as a substitute for the Reliability Standard or viewed as additional Reliability Standard requirements. In all cases, the Regional Entity should rely on the language contained in the Reliability Standard itself, and not on the language contained in this RSAW, to determine compliance with the Reliability Standard. NERC's Reliability Standards can be found on NERC's website. Additionally, NERC Reliability Standards are updated frequently, and this RSAW may not necessarily be updated with the same frequency. Therefore, it is imperative that entities treat this RSAW as a reference document only, and not as a substitute or replacement for the Reliability Standard. It is the responsibility of the registered entity to verify its compliance with the latest approved version of the Reliability Standards, by the applicable governmental authority, relevant to its registration status.

The RSAW may provide a non-exclusive list, for informational purposes only, of examples of the types of evidence a registered entity may produce or may be asked to produce to demonstrate compliance with the Reliability Standard. A registered entity's adherence to the examples contained within this RSAW does not necessarily constitute compliance with the applicable Reliability Standard, and NERC and the Regional Entity using this RSAW reserve the right to request additional evidence from the registered entity that is not included in this RSAW. This RSAW may include excerpts from FERC Orders and other regulatory references which are provided for ease of reference only, and this document does not necessarily include all applicable Order provisions. In the event of a discrepancy between FERC Orders, and the language included in this document, FERC Orders shall prevail.

[2] Compliance Assessment Date(s): The date(s) the actual compliance assessment (on-site audit, off-site spot check, etc.) occurs.

Findings

(This section to be completed by the Compliance Enforcement Authority)

Req.	Finding	Summary and Documentation	Functions Monitored
R1			

Req.	Areas of Concern

Req.	Recommendations

Req.	Positive Observations

Subject Matter Experts

Identify the Subject Matter Expert(s) responsible for this Reliability Standard.

Registered Entity Response (Required; Insert additional rows if needed):

SME Name	Title	Organization	Requirement(s)

Registered Entity Response (Required):

Question 1: Does the Registered Entity own or operate ~~a~~ an applicable Control Center? ☐ Yes ☐ No

If no:

1. Provide evidence in the space below that the Registered Entity does not own or operate ~~one or more~~an applicable Control Center~~s~~. This evidence may include, but is not limited to:
   - Evidence that the Registered Entity does not own or operate ~~a~~ an applicable Control Center; or
   - Evidence or a reference to evidence from the Registered Entity's CIP-002 compliance program that demonstrates the ~~entity~~ Registered Entity does not own or operate ~~a~~ an applicable Control Center.
2. The remainder of this RSAW may be left blank.

[Note: A separate spreadsheet or other document may be used. If so, provide the document reference below.]

R1 Supporting Evidence and Documentation

R1. The Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring data while being transmitted between any applicable Control Centers. The Responsible Entity is not required to include~~This requirement excludes~~ oral communications in its plan. The plan shall include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

- **1.1** Identification of security protection used to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers;
- **1.2** Identification of where the Responsible Entity applied security protection for transmitting Real-time Assessment and Real-time monitoring data between Control Centers; and
- **1.3** If the Control Centers are owned or operated by different Responsible Entities, identify the responsibilities of each Responsible Entity for applying security protection to the transmission of Real-time Assessment and Real-time monitoring data between those Control Centers.

M1. Evidence may include, but is not limited to, documented plan(s) that meet the security objective of Requirement R1 and documentation demonstrating the implementation of the plan(s).

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-012-1, R1

This section to be completed by the Compliance Enforcement Authority

	If the Registered Entity has answered "No" to Question 1, verify the Registered Entity does not own or operate an applicable Control Center. Note: If the Registered Entity does not own or operate an applicable Control Center, the remainder of this RSAW is not applicable.
	Verify the entity has implemented, except under CIP Exceptional Circumstances, one or more documented plan(s) to mitigate the risk of the unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring data while being transmitted between any applicable Control Centers.
	Verify the documented plans collectively include identification of security protection used to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring data while being transmitted between any applicable Control Centers.
	Verify the documented plans collectively include identification of where the Responsible Entity applied security protection for transmitting Real-time Assessment and Real-time monitoring data between any applicable Control Centers.
	If Real-time Assessment or Real-time monitoring data is transmitted between any applicable Control Centers owned or operated by different Responsible Entities, ~~V~~verify the documented plans collectively include identification of the responsibilities of each Responsible Entity for applying security protection to these transmissions~~the transmission of Real-time Assessment and Real-time monitoring data between Control Centers, when the Control Centers are owned or operated by different Responsible Entities~~.
	Verify the documented plans collectively achieve the security objective of mitigating the risk of the unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring data while being transmitted between any applicable Control Centers.
	If the Responsible Entity has declared and responded to CIP Exceptional Circumstances, verify the Responsible Entity has adhered to the applicable cyber security policies.
Notes to Auditor: 1. The Responsible Entity is not required to include oral communications in its plan.~~Oral communications are not in scope for CIP-012-1.~~ ~~1.~~2. See Applicability Section 4.2.3 for a decription of Control Centers that are exempt from this Standard.	

Auditor Notes:

Additional Information:

Reliability Standard

The full text of CIP-012-1 may be found on the NERC Web Site (www.nerc.com) under "Program Areas & Departments", "Standards," "Reliability Standards."

In addition to the Reliability Standard, there is an applicable Implementation Plan available on the NERC Web Site.

In addition to the Reliability Standard, there is background information available on the NERC Web Site.

Capitalized terms in the Reliability Standard refer to terms in the NERC Glossary, which may be found on the NERC Web Site.

Sampling Methodology

Sampling is essential for auditing compliance with NERC Reliability Standards since it is not always possible or practical to test 100% of either the equipment, documentation, or both, associated with the full suite of enforceable standards. The Sampling Guide contained in the Compliance Monitoring and Enforcement Manual (see NERC website) provided by the Electric Reliability Organization help to establish a minimum sample set for monitoring and enforcement uses in audits of NERC Reliability Standards.

Regulatory Language

FERC Order 822 P53-56, 58, and 62

Selected Glossary Terms

The following Glossary terms are provided for convenience only. Please refer to the NERC web site for the current enforceable terms.

CIP Exceptional Circumstance

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.

Control Center

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, of:

1) a Reliability Coordinator,
2) a Balancing Authority,
3) a Transmission Operator for transmission Facilities at two or more locations, or
4) a Generator Operator for generation Facilities at two or more locations.

~~One or more facilities, including their associated data centers, that monitor and control the Bulk Electric System (BES) and also host operating personnel who:~~

~~1) perform the Real-time reliability-related tasks of a Reliability Coordinator; or~~
~~2) perform the Real-time reliability-related tasks of a Balancing Authority; or~~
~~3) perform the Real-time reliability-related tasks of a Transmission Operator for Transmission Facilities at two or more locations; or~~
~~4) can act independently as the Generator Operator to develop specific dispatch instructions for generation Facilities at two or more locations; or~~
~~5) can operate or direct the operation of a Transmission Owner's BES Transmission Facilities in Real-time.~~

~~Operating personnel do not include:~~
~~1) plant operators located at a generator plant site or personnel at a centrally located dispatch center who relay dispatch instructions without making any modifications; or~~
~~2) Transmission Owner or Transmission Operator field switching personnel.~~

Real-time Assessment
An evaluation of system conditions using Real-time data to assess existing (pre-Contingency) and potential (post-Contingency) operating conditions. The assessment shall reflect applicable inputs including, but not limited to: load, generation output levels, known Protection System and Special Protection System status or degradation, Transmission outages, generator outages, Interchange, Facility Ratings, and identified phase angle and equipment limitations. (Real-time Assessment may be provided through internal systems or through third-party services.)

Real-time
Present time as opposed to future time.

Revision History for RSAW

Version	Date	Reviewers	Revision Description
Draft1 v1	07/28/2017	NERC Stds Group	New document
Draft1 v2	08/01/2017	RSAW Task Force	Modified Question to clarify applicability
Draft1 v3	08/02/2017	RSAW Task Force	Response to MRO comments. Moved Questions 1 and 2 above R1. Made text changes to Q1 and to R2 Compliance Assessment Approach.
Draft1 v4	08/07/2017	RSAW Task Force, 2016-02 SDT	Response to TexasRE and SDT comments. Clarified scope of Q1 to be data transmitted between Control Centers. Removed extra space from Auditor Notes.
Draft2 v1	10/27/2017	RSAW Task Force	Modified title. Modified Q2 to conform with new language. Modified R1 with new Requirement text and new Compliance Assessment Approach. Modified R2 with new Compliance Assessment Approach. Removed Operational Planning Analysis from the Selected Glossary Terms. Modified footer with revised version and date.
Draft2 v2	11/27/2017	RSAW Task Force, Standard Drafting Team	Response to comments: • RF: Footnote 1 page 1 added space after "references." • RF: Changed "Tasf" to "Task" in Revision History. • Response to SERC CIPC and Southern Company comments to Draft 1. • Modified Question 1 to include reference to CIP-002. • Added an item to the R1 Compliance Assessment Approach to verify the effectiveness of the process. • Modified the R2 Compliance Assessment Approaches to clarify that the review is for implementation.
Draft3 v0	03/20/2018	RSAW Task Force	Modified for Draft 3 language: • Removed Requirement R2 • Modified Requirement R1 language to match the Standard • Modified the R1 Compliannce Assessment Approach

			• Removed "CIP Exceptional Circumstance" from the Selected Glossary Terms • Revised the definition of "Control Center" in Selected Glossary Terms to match the definition posted alongside CIP-012-1 Draft 3
Draft3 v1	04/03/2018	ERO Enterprise	• Consideration of Comments from RF o Changed Sampling Methodology section to match current NERC documents. Will also need to be reflected in the RSAW Template.
Draft3 v2	4/25/2018	NERC Legal	Addressed comments. No text changes were made.
Draft4 v0	5/19/2018	RSAW Task Force	Modified for Draft 4 language: • Modified Question 1 to reference "applicable" Control Centers • Modified Requirement R1 language to match the Standard • Modified the R1 Compliance Assessment Approach • Modified the Note to Auditor in Compliance Assessment Approach • Restored the definition of "CIP Exceptional Circumstance" to the Selected Glossary Terms • Restored the approved definition of "Control Center" to the Selected Glossary Terms
Draft4 v1	6/4/2018	RSAW Task Force	Modified language of Question 1 to more closely match the Standard.
Draft4 v2	6/11/2018	NERC Compliance /NERC Legal	Addressed corrections/comments from NERC: • Corrected "entity" to "Registered Entity" in Question 1 • Addressed question regarding use of (s) in certain cases • Corrected "of responsibilities" to "of the responsibilities" in CAA item 5 • Addressed comment regarding CAA item 5 • Addressed comment regarding additional Note to Auditor • Removed underlining from definition of Control Center

			• Inserted hyphen into real-time in Control Center definition • Added “any applicable” Control Center to CAA items 3, 4, and 6.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2016-02 Modifications to CIP Standards

Formal Comment Period Open through July 2, 2018

Now Available

A 45-day formal comment period for **CIP-012-1 – Cyber Security - Communications between Control Centers** is open through **8 p.m. Eastern, Monday, July 2, 2018.**

The Technical Rationale and Implementation Guidance Documents for CIP-012-1 will be posted within 15 days of the comment period opening.

Additionally, the CIP standard drafting team (SDT) proposed a revised Control Center definition during the March 16 – April 30, 2018 comment and ballot period. Based on feedback received from industry, the SDT decided to draft exemption language within the applicability section of CIP-012 instead of revising the Control Center definition. Please see the Control Center definition consideration of comments report for additional SDT responses on the new path taken by the SDT.

Commenting

Use the Standards Balloting and Commenting System (SBS) to submit comments. If you experience difficulties navigating the SBS, contact Wendy Muller. An unofficial Word version of the comment form is posted on the project page.

- *If you are having difficulty accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out, contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern).*
- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*
- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Next Steps

An additional ballot for the Standard and a non-binding poll of the associated Violation Risk Factors and Violation Severity Levels will be conducted **June 22 – July 2, 2018.**

For information on the Standards Development Process, refer to the Standard Processes Manual**.**

For more information or assistance, contact Standards Developer, Jordan Mallory at (404) 446-2589.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Comment Report

Project Name:	2016-02 Modifications to CIP Standards | CIP-012-1 Draft 4
Comment Period Start Date:	5/18/2018
Comment Period End Date:	7/3/2018
Associated Ballots:	2016-02 Modifications to CIP Standards CIP-012-1 AB 4 ST

There were 55 sets of responses, including comments from approximately 149 different people from approximately 101 companies representing 10 of the Industry Segments as shown in the table on the following pages.

Questions

1. Control Center Exemption Language: The SDT drafted Exemption language in the Applicability section specifically for CIP-012-1 to exempt Control Centers that only transmit data pertaining to a single co-located substation or generating plant. Do you agree with this revision? If not, please provide the basis for your disagreement and an alternate proposal.

2. Requirement R1: The SDT modified Requirement R1 to state: "The Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring data while being transmitted between any applicable Control Centers. The Responsible Entity is not required to include oral communications in its plan." Do you agree with this revision? If not, please provide the basis for your disagreement and an alternate proposal.

3. Implementation Plan: The SDT established the Implementation Plan to make the standard effective the first day of the first calendar quarter that is twenty-four (24) calendar months after the effective date of the applicable governmental authority's order approving the standard, or as otherwise provided for by the applicable governmental authority. Do you agree with this proposal? If you think an alternate implementation time period is needed, please provide a detailed explanation of actions and time needed to meet the implementation deadline.

4. Technical Rationale: The SDT modified the draft Technical Rationale for CIP-012 to further explain the need for the exemption for certain Control Centers. Do you agree with the explanations and included diagrams in the draft Technical Rationale? If you do not agree, or if you agree but have comments or suggestions for the draft Technical Rationale, please provide your recommendation and explanation.

5. The SDT modified the draft Implementation Guidance for CIP-012 to provide examples of how a Responsible Entity could comply with the requirements. The draft Implementation Guidance does not prescribe the only approaches to compliance. Rather, it describes what the SDT believes would be effective ways to comply with the standard. See NERC's Compliance Guidance policy for information on Implementation Guidance. Do you agree with the draft Implementation Guidance? If you do not agree, or if you agree but have comments or suggestions for the draft Implementation Guidance, please provide your recommendation and explanation.

6. The SDT believes proposed CIP-012-1 provides entities with flexibility to meet the reliability objectives in a cost effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost effective approaches, please provide your recommendation and, if appropriate, technical justification.

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim	3	RF	FirstEnergy Corporation	Aaron Ghdooshim	FirstEnergy - FirstEnergy Corporation	4	RF
					Aubrey Short	FirstEnergy - FirstEnergy Corporation	1	RF
					Theresa Ciancio	FirstEnergy - FirstEnergy Corporation	3	RF
					Robert Loy	FirstEnergy - FirstEnergy Solutions	5	RF
					Ann Ivanc	FirstEnergy - FirstEnergy Solutions	6	RF
Brandon McCormick	Brandon McCormick		FRCC	FMPA	Tim Beyrle	City of New Smyrna Beach Utilities Commission	4	FRCC
					Jim Howard	Lakeland Electric	5	FRCC
					Lynne Mila	City of Clewiston	4	FRCC
					Javier Cisneros	Fort Pierce Utilities Authority	3	FRCC
					Randy Hahn	Ocala Utility Services	3	FRCC
					Don Cuevas	Beaches Energy Services	1	FRCC
					Jeffrey Partington	Keys Energy Services	4	FRCC
					Tom Reedy	Florida Municipal Power Pool	6	FRCC
					Steven Lancaster	Beaches Energy Services	3	FRCC

					Mike Blough	Kissimmee Utility Authority	5	FRCC
					Chris Adkins	City of Leesburg	3	FRCC
					Ginny Beigel	City of Vero Beach	3	FRCC
Santee Cooper	Chris Wagner	1		Santee Cooper	Rene' Free	Santee Cooper	1,3,5,6	SERC
					Rodger Blakely	Santee Cooper	1,3,5,6	SERC
					Troy Lee	Santee Cooper	1,3,5,6	SERC
					Jennifer Richards	Santee Cooper	1,3,5,6	SERC
					Chris Jimenez	Santee Cooper	1,3,5,6	SERC
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
MRO	Dana Klem	1,2,3,4,5,6	MRO	MRO NSRF	Joseph DePoorter	Madison Gas & Electric	3,4,5,6	MRO
					Larry Heckert	Alliant Energy	4	MRO
					Amy Casucelli	Xcel Energy	1,3,5,6	MRO
					Michael Brytowski	Great River Energy	1,3,5,6	MRO
					Jodi Jensen	Western Area Power Administration	1,6	MRO
					Kayleigh Wilkerson	Lincoln Electric System	1,3,5,6	MRO
					Mahmood Safi	Omaha Public Power District	1,3,5,6	MRO
					Brad Parret	Minnesota Powert	1,5	MRO
					Terry Harbour	MidAmerican Energy Company	1,3	MRO

					Tom Breene	Wisconsin Public Service Corporation	3,5,6	MRO
					Jeremy Voll	Basin Electric Power Cooperative	1	MRO
					Kevin Lyons	Central Iowa Power Cooperative	1	MRO
					Mike Morrow	Midcontinent ISO	2	MRO
Southern Company - Southern Company Services, Inc.	Pamela Hunter	1,3,5,6	SERC	Southern Company	Katherine Prewitt	Southern Company Services, Inc.	1	SERC
					Joel Dembowski	Southern Company - Alabama Power Company	3	SERC
					William D. Shultz	Southern Company Generation	5	SERC
					Jennifer G. Sykes	Southern Company Generation and Energy Marketing	6	SERC
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,8,9,10	NPCC	RSC no Dominion	Guy V. Zito	Northeast Power Coordinating Council	10	NPCC
					Randy MacDonald	New Brunswick Power	2	NPCC
					Wayne Sipperly	New York Power Authority	4	NPCC
					Glen Smith	Entergy Services	4	NPCC
					Brian Robinson	Utility Services	5	NPCC
					Alan Adamson	New York State Reliability Council	7	NPCC

Edward Bedder	Orange & Rockland Utilities	1	NPCC
David Burke	Orange & Rockland Utilities	3	NPCC
Michele Tondalo	UI	1	NPCC
Laura Mcleod	NB Power	1	NPCC
David Ramkalawan	Ontario Power Generation Inc.	5	NPCC
Helen Lainis	IESO	2	NPCC
Michael Schiavone	National Grid	1	NPCC
Michael Jones	National Grid	3	NPCC
Michael Forte	Con Ed - Consolidated Edison	1	NPCC
Peter Yost	Con Ed - Consolidated Edison Co. of New York	3	NPCC
Sean Cavote	PSEG	4	NPCC
Kathleen Goodman	ISO-NE	2	NPCC
Paul Malozewski	Hydro One Networks, Inc.	3	NPCC
Quintin Lee	Eversource Energy	1	NPCC
Dermot Smyth	Con Ed - Consolidated Edison Co. of New York	1,5	NPCC
Dermot Smyth	Con Ed - Consolidated Edison Co. of New York	1,5	NPCC
Salvatore Spagnolo	New York Power Authority	1	NPCC
Shivaz Chopra	New York Power Authority	6	NPCC

					David Kiguel	Independent	NA - Not Applicable	NPCC
					Silvia Mitchell	NextEra Energy - Florida Power and Light Co.	6	NPCC
					Caroline Dupuis	Hydro Quebec	1	NPCC
					Chantal Mazza	Hydro Quebec	2	NPCC
					Gregory Campoli	New York Independent System Operator	2	NPCC
Southwest Power Pool, Inc. (RTO)	Shannon Mickens	2	MRO,SPP RE	SPP Standards Review Group	Shannon Mickens	Southwest Power Pool Inc.	2	MRO
					Don Schmit	Nebraska Public Power District	5	NA - Not Applicable
					John Allen	City Utilities of Springfield, Missouri	4	MRO
					Louis Guidry	Cleco	1,3,5,6	SERC
					Robert Gray	Board of Public Utilities (Kansas City, KS) BPU	3	MRO
					Steven Keller	Southwest Power Pool Inc.	2	MRO
PPL - Louisville Gas and Electric Co.	Shelby Wade	1,3,5,6	RF,SERC	PPL NERC Registered Affiliates	Charlie Freibert	LG&E and KU Energy, LLC	3	SERC
					Brenda Truhe	PPL Electric Utilities Corporation	1	RF
					Dan Wilson	LG&E and KU Energy, LLC	5	SERC
					Linn Oelker	LG&E and KU Energy, LLC	6	SERC
Associated Electric Cooperative, Inc.	Todd Bennett	3		AECI	Michael Bax	Central Electric Power Cooperative (Missouri)	1	SERC
					Adam Weber	Central Electric Power	3	SERC

	Cooperative (Missouri)		
Stephen Pogue	M and A Electric Power Cooperative	3	SERC
William Price	M and A Electric Power Cooperative	1	SERC
Jeff Neas	Sho-Me Power Electric Cooperative	3	SERC
Peter Dawson	Sho-Me Power Electric Cooperative	1	SERC
Mark Ramsey	N.W. Electric Power Cooperative, Inc.	1	NPCC
John Stickley	NW Electric Power Cooperative, Inc.	3	SERC
Ted Hilmes	KAMO Electric Cooperative	3	SERC
Walter Kenyon	KAMO Electric Cooperative	1	SERC
Kevin White	Northeast Missouri Electric Power Cooperative	1	SERC
Skyler Wiegmann	Northeast Missouri Electric Power Cooperative	3	SERC
Ryan Ziegler	Associated Electric Cooperative, Inc.	1	SERC
Brian Ackermann	Associated Electric Cooperative, Inc.	6	SERC
Brad Haralson	Associated Electric Cooperative, Inc.	5	SERC

1. Control Center Exemption Language: The SDT drafted Exemption language in the Applicability section specifically for CIP-012-1 to exempt Control Centers that only transmit data pertaining to a single co-located substation or generating plant. Do you agree with you revision? If not, please provide the basis for your disagreement and an alternate proposal.

Russell Martin II - Salt River Project - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

SRP agrees with the principal of the exemption. However, SRP would like to see a revision of the language simplified in a fashion similar to how this question is constructed. "exempt Control Centers that only transmit data pertaining to a single-co-located substation or generation plant."

Likes 0	
Dislikes 0	

Response

Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	No
Document Name	

Comment

The Technical Rationale document, in addressing this exemption, identifies the “intent” of this exemption which is to “exclude the normal RTU-style communication from a field asset about that field asset’s status from CIP-012”. This is commendable and the NSRF appreciates your identification of RTU-style communication as an exemption as it relates to the Control Center definition. The NSRF would like to point out that there are violations of Standards that have come down to discussions over intent. The NSRF strongly suggests that the drafting team include the Technical Rationale intent for this exemption into the actual words of the exemption to avoid future misinterpretation of the exemption. NSRF suggests the following for drafting team consideration, which also includes revisions for comments under #4 of this comment form:

The NSRF recommends that the exemption reads as:

A Control Center at a **BES** generation resource or Transmission station or substation that transmits to another Control Center Real-time Assessment or Real-time monitoring data**, such as RTU-style data,** pertaining only to the generation resource or Transmission station or substation at which the **data** transmitting **transmitted** Control Center is located.

Rationale: The first use of “Control Center” implies that the exemption is for a Control Center to start with. Where it is not a Control Center but a BES facility that transmits data, via an RTU (RTU was added since it plays a pivotal point of intent within the Technical Rational document).

Likes 0	
Dislikes 0	

Response

Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	No
Document Name	
Comment	
The exemption language of CIP-012-1 4.2.3 refers to real-time data derived from a **single** location at a generation or Transmission station. However, the Control Center term, as defined In the Proposed Definition of Control Center, items (3) and (4), refers to "**two or more locations**" for Transmission Operators and Generator Operators. They are conflicting one another and this could lead to misinterpretation and/or misapplication of the Standard's protections. WECC believe clarity related to control Center vs. control room is necessary.	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	No
Document Name	
Comment	
Language is very confusing. Based on Idaho Power's understanding, this will eliminate smaller Control Centers but doesn't appear to have a large impact.	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 1,3,6	
Answer	No
Document Name	
Comment	
While Ameren supports the need for an Exemption for CIP-012-1, the exemption should be based on impact to reliable operations. We suggest modifying the proposed wording in 4.2.3 to provide the exemption for Low Impact Control Centers as defined in CIP-002, Attachment 1. If a Control Center regardless of its location meets the criteria for either a Medium Impact or High Impact facility then it should be protected appropriately.	
Likes 0	
Dislikes 0	

Response	
Aaron Smith - Omaha Public Power District - 1,3,5,6	
Answer	No
Document Name	
Comment	

The Technical Rationale document, in addressing this exemption, identifies the “intent” of this exemption which is to “exclude the normal RTU-style communication from a field asset about that field asset’s status from CIP-012”. This is commendable and the NSRF appreciates your identification of RTU-style communication as an exemption as it relates to the Control Center definition. The NSRF would like to point out that there are violations of Standards that have come down to discussion over intent; and the NSRF strongly suggests that the drafting team include the Technical Rationale intent for this exemption into the actual words of the exemption to avoid future misinterpretation of the exemption. NSRF suggests the following for drafting team consideration, which also includes revisions for comments under #4 of this comment form:

The NSRF recommends that the exemption reads as:

A Control Center at a **BES** generation resource or Transmission station or substation that transmits to a nother Control Center Real-time Assessment or Real-time monitoring

Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	No
Document Name	
Comment	

Reclamation does not support an exemption. Reclamation recommends that all Real-time Assessment and Real-time monitoring data be protected against the risk of unauthorized disclosure or modification.

Instead of exempting certain Control Centers, Reclamation recommends the SDT revise the Control Center definition to give consideration to the system-wide view a Control Center has versus the limited view held by Generator Operators as follows:

One or more BES facilities, including their associated Data Centers, that monitor and control the BES and also host System Operators who:

1. perform the Real-time reliability-related tasks of a Reliability Coordinator; or
2. perform the Real-time reliability-related tasks of a Balancing Authority; or

3. perform the Real-time reliability-related tasks of a Transmission Operator for any BES Transmission Facilities; or

4. can act independently as the Generator Operator to develop specific dispatch instructions for any BES generation Facilities; or

5. can operate or direct the operation of a Transmission Owner's BES Transmission Facilities in Real-time.

Section 4.2.3, as presently written, does not clearly explain why certain Control Centers would be exempted. If an exemption is provided, Reclamation recommends the SDT incorporate language from the Technical Rationale in the exemption to avoid future confusion (i.e., Control Center implies the exemption is for a Control Center, but the data may be transmitted by a BES facility such as an RTU).

Likes 0	
Dislikes 0	

Response

Brandon McCormick - Brandon McCormick On Behalf of: Ginny Beigel, City of Vero Beach, 3; Lynne Mila, City of Clewiston, 4; Mike Blough, Kissimmee Utility Authority, 5, 3; Tom Reedy, Florida Municipal Power Pool, 6; - Brandon McCormick, Group Name FMPA

Answer	No
Document Name	

Comment

: FMPA agrees with the following comments submitted by MRO NSRF:

The Technical Rationale document, in addressing this exemption, identifies the "intent" of this exemption which is to "exclude the normal RTU-style communication from a field asset about that field asset's status from CIP-012". This is commendable and the NSRF appreciates your identification of RTU-style communication as an exemption as it relates to the Control Center definition. The NSRF would like to point out that there are violations of Standards that have come down to discussions over intent. The NSRF strongly suggests that the drafting team include the Technical Rationale intent for this exemption into the actual words of the exemption to avoid future misinterpretation of the exemption. NSRF suggests the following for drafting team consideration, which also includes revisions for comments under #4 of this comment form:

The NSRF recommends that the exemption reads as:

A Control Center at a **BES** generation resource or Transmission station or substation that transmits to another Control Center Real-time Assessment or Real-time monitoring data**, such as RTU-style data,** pertaining only to the generation resource or Transmission station or substation at which the **data** transmitting **transmitted** Control Center is located.

Rationale: The first use of "Control Center" implies that the exemption is for a Control Center to start with. Where it is not a Control Center but a BES facility that transmits data, via an RTU (RTU was added since it plays a pivotal point of intent within the Technical Rational document)

Likes 0	
Dislikes 0	

Response

Douglas Webb - Douglas Webb On Behalf of: Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; James McBee, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; Jessica Tucker, Great Plains Energy - Kansas City Power and Light Co., 5,

1, 3, 6; Jim Flucke, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; Megan Wagner, Westar Energy, 6, 3, 1, 5; - Douglas Webb	
Answer	No
Document Name	
Comment	
Kansas City Power and Light Company incorporates the Edison Electric Institute's response to Question No. 1.	
Likes 0	
Dislikes 0	
Response	
Richard Montgomery - Florida Municipal Power Agency - 3,4,5,6	
Answer	No
Document Name	
Comment	
FMPA agrees with the following comments submitted by MRO NSRF: The Technical Rationale document, in addressing this exemption, identifies the “intent” of this exemption which is to “exclude the normal RTU-style communication from a field asset about that field asset’s status from CIP-012”. This is commendable and the NSRF appreciates your identification of RTU-style communication as an exemption as it relates to the Control Center definition. The NSRF would like to point out that there are violations of Standards that have come down to discussions over intent. The NSRF strongly suggests that the drafting team include the Technical Rationale intent for this exemption into the actual words of the exemption to avoid future misinterpretation of the exemption. NSRF suggests the following for drafting team consideration, which also includes revisions for comments under #4 of this comment form: The NSRF recommends that the exemption reads as: A Control Center at a **BES** generation resource or Transmission station or substation that transmits to another Control Center Real-time Assessment or Real-time monitoring data**, such as RTU-style data,** pertaining only to the generation resource or Transmission station or substation at which the **data** transmitting **transmitted** Control Center is located. Rationale: The first use of “Control Center” implies that the exemption is for a Control Center to start with. Where it is not a Control Center but a BES facility that transmits data, via an RTU (RTU was added since it plays a pivotal point of intent within the Technical Rational document)	
Likes 0	
Dislikes 0	
Response	
Carol Chinn - Florida Municipal Power Agency - 3,4,5,6	
Answer	No

Document Name	

Comment

FMPA agrees with the following comments submitted by MRO NSRF:

The Technical Rationale document, in addressing this exemption, identifies the “intent” of this exemption which is to “exclude the normal RTU-style communication from a field asset about that field asset’s status from CIP-012”. This is commendable and the NSRF appreciates your identification of RTU-style communication as an exemption as it relates to the Control Center definition. The NSRF would like to point out that there are violations of Standards that have come down to discussions over intent. The NSRF strongly suggests that the drafting team include the Technical Rationale intent for this exemption into the actual words of the exemption to avoid future misinterpretation of the exemption. NSRF suggests the following for drafting team consideration, which also includes revisions for comments under #4 of this comment form:

The NSRF recommends that the exemption reads as:

A Control Center at a **BES** generation resource or Transmission station or substation that transmits to another Control Center Real-time Assessment or Real-time monitoring data**, such as RTU-style data,** pertaining only to the generation resource or Transmission station or substation at which the **data** transmitting **transmitted** Control Center is located.

Rationale: The first use of “Control Center” implies that the exemption is for a Control Center to start with. Where it is not a Control Center but a BES facility that transmits data, via an RTU (RTU was added since it plays a pivotal point of intent within the Technical Rational document)

Likes 0	
Dislikes 0	

Response

Joe McKinney - Florida Municipal Power Agency - 3,4,5,6

Answer	No
Document Name	

Comment

FMPA agrees with the following comments submitted by MRO NSRF:

The Technical Rationale document, in addressing this exemption, identifies the “intent” of this exemption which is to “exclude the normal RTU-style communication from a field asset about that field asset’s status from CIP-012”. This is commendable and the NSRF appreciates your identification of RTU-style communication as an exemption as it relates to the Control Center definition. The NSRF would like to point out that there are violations of Standards that have come down to discussions over intent. The NSRF strongly suggests that the drafting team include the Technical Rationale intent for this exemption into the actual words of the exemption to avoid future misinterpretation of the exemption. NSRF suggests the following for drafting team consideration, which also includes revisions for comments under #4 of this comment form:

The NSRF recommends that the exemption reads as:

A Control Center at a **BES** generation resource or Transmission station or substation that transmits to another Control Center Real-time Assessment or Real-time monitoring data**, such as RTU-style data,** pertaining only to the generation resource or Transmission station or substation at which the **data** transmitting **transmitted** Control Center is located.

Rationale: The first use of “Control Center” implies that the exemption is for a Control Center to start with. Where it is not a Control Center but a BES facility that transmits data, via an RTU (RTU was added since it plays a pivotal point of intent within the Technical Rational document)

Likes 0	
Dislikes 0	

Response

Chris Gowder - Florida Municipal Power Agency - 3,4,5,6

Answer	No
Document Name	

Comment

Comments**:** FMPA agrees with the following comments submitted by MRO NSRF:

The Technical Rationale document, in addressing this exemption, identifies the “intent” of this exemption which is to “exclude the normal RTU-style communication from a field asset about that field asset’s status from CIP-012”. This is commendable and the NSRF appreciates your identification of RTU-style communication as an exemption as it relates to the Control Center definition. The NSRF would like to point out that there are violations of Standards that have come down to discussions over intent. The NSRF strongly suggests that the drafting team include the Technical Rationale intent for this exemption into the actual words of the exemption to avoid future misinterpretation of the exemption. NSRF suggests the following for drafting team consideration, which also includes revisions for comments under #4 of this comment form:

The NSRF recommends that the exemption reads as:

A Control Center at a **BES** generation resource or Transmission station or substation that transmits to another Control Center Real-time Assessment or Real-time monitoring data**, such as RTU-style data,** pertaining only to the generation resource or Transmission station or substation at which the **data** transmitting **transmitted** Control Center is located.

Rationale: The first use of “Control Center” implies that the exemption is for a Control Center to start with. Where it is not a Control Center but a BES facility that transmits data, via an RTU (RTU was added since it plays a pivotal point of intent within the Technical Rational document

Likes 0	
Dislikes 0	

Response

Chris Scanlon - Exelon - 1

Answer	No
Document Name	CIP 12 Figures.pdf

Comment

While Exelon supports the need for an Exemption for CIP-012-1, we have a concern that the language may still lack necessary clarity. For this reason, we suggest language similar to the following:

4.2.3 A generating station, Transmission station or substation that is also a Control Center, but meets one of the following criteria:

4.2.3.1 Aggregates and transmits Real-time Assessment and Real-time monitoring data from two or more Generation resource(s), Transmission station(s) and/or substation(s) but all aggregated data coming from these locations is contained within the same physical perimeter. (see Figure 1)

4.2.3.2 Does not aggregate and transmit Real-time Assessment and Real-time monitoring data from a location outside the physical perimeter where it resides. (see Figure 2)

(See CIP 12 Figures.pdf)

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

The Exemption Language is ambiguous with regard to situations where an entity could have BES assets polling Non-BES data from other locations/facilities.

Example 1: Weather Data from remote locations. No effect on generation but weather station is not physically at this facility.

Example 2: Operations of small hydro sites (under 10 mw) which are aggregated at the Low Impact BES facility but are located at other facilities.

In this example, these Low Impact Control Centers are only identified as Control Centers because they have the Capability, NOT the Responsibility, to control another Low Impact BES site. The capability is there so that technicians at one site can monitor alarms at the other Low Impact site. But these sites are not staffed around the clock, and their function is not to perform operations at the other site. We suggest a clarification on the exemption language below.

Current Language:

A Control Center at a generation resource or Transmission station or substation that transmits to another Control Center Real-time Assessment or Real-time monitoring data pertaining only to the generation resource or Transmission station or substation at which the transmitting Control Center is located.

Language Suggestion:

A Control Center at a generation resource or Transmission station or substation where all of the BES data being transmitted to another Control Center, pertains to the generation resource or Transmission station or substation at which the transmitting Control Center is located.

This language is intended to prevent small sites with Non BES data coming from other locations from being unnecessarily included in the standard.

Likes 0	
Dislikes 0	

Response
Stephanie Burns - Stephanie Burns On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Stephanie Burns

Answer	No
Document Name	

Comment
ITC is concerned with the use of Control Center in the exemption and the confusion it may cause with the originally intended definition of Control Center. ITC instead recommends the following language: Exemption: BES generation resource or Transmission station or substation that transmits Realtime monitoring or Assessment data to another Control Center, such as telemetry data, pertaining only to the generation resource or Transmission station.

Likes 0	
Dislikes 0	

Response
Eli Rivera - Central Electric Cooperative, Inc. (Redmond, Oregon) - NA - Not Applicable - Texas RE

Answer	No
Document Name	

Comment
CenterPoint Energy Houston Electric, LLC (“CenterPoint Energy”) agrees with Edison Electric Institute’s (EEI) comments.

Likes 0	
Dislikes 0	

Response
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman

Answer	No
Document Name	

Comment
Please refer to MRO NERC Standards Review Forum (NSRF) comments.

Likes 0	
Dislikes 0	

Response

Shelby Wade - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates

Answer	No
Document Name	

Comment

Under the current definition of Control Center per the NERC Glossary of terms, what qualifies as an associated data center is unclear (e.g., associated computer room, remote computer room, distributed front-end processor).

PPL NERC Registered Affiliates requests clarification regarding treatment of aggregation of SCADA data, in particular:

- Please provide additional information and a diagram for the scope and exemptions for SCADA data from multiple substations to a remote computer room where data is aggregated at the remote computer room prior to transmitting to a data center that is associated with the Operations Center.
- Please provide additional information and a diagram regarding communications scope of CIP-012-1 (e.g. SCADA data from various substation control buildings that are at a single location and communicating back via a network used for all substation communications back to head end computer room, aggregated and then sent to Data Center).

Likes 0	
Dislikes 0	

Response

Andrea Koch - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	No
Document Name	CIP 12 Figures.pdf

Comment

While EEI supports the need for an Exemption for CIP-012-1, we are concerned that the language may still lack necessary clarity. For this reason, we suggest language similar to the following:

4.2.3 A generating station, Transmission station or substation that is also a Control Center, but meets one of the following criteria:

4.2.3.1 Aggregates and transmits Real-time Assessment and Real-time monitoring data from two or more Generation resource(s), Transmission station(s) and/or substation(s) but all aggregated data comes from locations that are contained within the same physical perimeter. (see EEI Figure 1)

4.2.3.2 The Control Center does not aggregate and transmit Real-time Assessment and Real-time monitoring data from location(s) outside the physical perimeter where it resides. (see EEI Figure 2)

Likes 0	

Dislikes 0	
Response	
Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran	
Answer	No
Document Name	
Comment	
Oncor supports EEI's comment.	
Likes 0	
Dislikes 0	
Response	
Warren Cross - ACES Power Marketing - 1,3,4,5 - MRO,WECC,Texas RE,SERC	
Answer	No
Document Name	
Comment	
The intent of the exclusion is a positive direction, but it needs re-worded for clarity. ACES is concerned that by identifying the facility as a NERC defined, Control Center, and not a NERC defined, Facility, it will have unintended consequences of being in scope to other standards that do not directly exempt it as a Control Center. ACES would support the following modification: “A BES generation resource or Transmission station or substation that transmits Real-time Assessment or Real-time monitoring data via RTU to a Control Center, and the transmitted data pertains only to that generation resource or Transmission station or substation.”	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - MRO, Group Name SPP Standards Review Group	
Answer	No
Document Name	

Comment
The SPP Standards Review Group has a concern that the proposed Exemption will modify the current “Control Center” definition that potentially changes how High and Low impacts assets are evaluated. The review group is proposing some language (shown below) to help maintain consistency with the “Control Center” Definition and the proposed Exemption mentioned in the documentation. Additionally, the introduction of the term “Control System” as well as the diagrams and explanations in the rationale present complexity pertaining to the current process of identifying BES Cyber Systems. We would suggest that the drafting team remove the term “Control System” from all proposed language associated with this project. Section 4.2.3. (Applicability Section –Standard) A **BES** generation resource or Transmission station or substation that transmits to a Control Center Real-time Assessment or Real-time monitoring data**, such as RTU-style data,** pertaining only to the generation resource or Transmission station or substation at which the **data transmitted** is located.

Likes 0	
Dislikes 0	

Response

Teresa Cantwell - Lower Colorado River Authority - 1,5	
Answer	Yes
Document Name	

Comment
None.

Likes 0	
Dislikes 0	

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	

Comment
PacifiCorp agrees with the SDT providing the exemption language within the standard coupled with the clarification provided in the technical rationale document in the absence of revising the Control Center definition. If additional edits to the exemption language changes the scope of what is covered in the final version or is the technical rationale is not ERO-endorsed prior to the final ballot, PacifiCorp may alter its final vote. PAC understands that time and the SAR are obstacles for the SDT at this time, further development of the Control Center definition should be resolved before more standards regarding Control Centers are introduced.

Likes 0	

Dislikes 0	

Response

Darnez Gresham - Darnez Gresham On Behalf of: Annette Johnston, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Darnez Gresham	
Answer	Yes
Document Name	

Comment
MEC agrees with the SDT providing the exemption language in the applicability of the standard coupled with the explanation in the technical rationale document in the absence of revising the Control Center definition. If additional edits to the exemption language changes the scope of what is covered in the final version, MEC will change its vote on the final ballot. MEC understands that time and the SAR are obstacles for the SDT at this time, however, issues with the existing Control Center definition should be resolved before more standards regarding Control Centers are introduced.

Likes 0	
Dislikes 0	

Response

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	

Comment
NV Energy agrees with the SDT providing the exemption language within the standard coupled with the clarification provided in the technical rationale document in the absence of revising the Control Center definition. Please note, that NV Energy may alter its vote, If additional edits to the exemption language changes the scope of what is covered in the final version or if the technical rationale is not ERO-endorsed prior to the final ballot. NV Energy understands that a unknown expedited timeline and the original SAR are obstacles for the SDT at this time, and that this Standard will be approved in the near term, but we believe that further development of the Control Center definition should be resolved before more standards regarding Control Centers are introduced.

Likes 0	
Dislikes 0	

Response

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	

Comment	
None	
Likes 0	
Dislikes 0	
Response	
Marty Hostler - Northern California Power Agency - 5	
Answer	Yes
Document Name	
Comment	
What about a similar Control Center that also receives data?	
Likes 0	
Dislikes 0	
Response	
Dennis Sismaet - Northern California Power Agency - 6	
Answer	Yes
Document Name	
Comment	
What about a similar Control Center that also receives data?	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	

Southern Company supports the proposed exemption language.	
Likes 0	
Dislikes 0	
Response	
David Francis - Midcontinent ISO, Inc. - 2 - MRO,SERC,RF	
Answer	Yes
Document Name	
Comment	
Adding the wording "within the same geographical location" might help with the clarification of located	
Likes 0	
Dislikes 0	
Response	
Steve Rose - City Water, Light and Power of Springfield, IL - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thomas Foltz - AEP - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aubrey Short - FirstEnergy - FirstEnergy Corporation - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 3, Group Name FirstEnergy Corporation	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
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	
David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Shaw - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeff Johnson - Jeff Johnson On Behalf of: Martine Blair, Sempra - San Diego Gas and Electric, 3, 5, 1; - Jeff Johnson	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Douglas Johnson - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Anderson - CMS Energy - Consumers Energy Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Wagner - Santee Cooper - 1, Group Name Santee Cooper	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Martin Sidor - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Greyerbiehl - CMS Energy - Consumers Energy Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 3	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Steven Mavis - Edison International - Southern California Edison Company - 1	
Answer	
Document Name	
Comment	
Please see comments submitted by Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	

While the SDT believes the “integrity and availability of sensitive bulk electric system data”, as noted in FERC Order No. 822, paragraph 54, is addressed in R1, Texas RE notes the use of the term “or”: Identification of security protection used to mitigate the risk of unauthorized disclosure *or* modification of Real-time Assessment and Real-time monitoring and control data while being transmitted between Control Centers. In its response, the SDT specifically referenced the Consideration of Issue or Directive document. In that document, the SDT makes clear that entities may elect, solely at their discretion, to protect communications links, data, or both.

Texas RE believes this directly conflicts with the plain language in FERC Order No. 822, P. 54. FERC made it clear that protections should apply to both communication links and sensitive data. However, the SDT has specified such protections could be potentially applied solely to communications links or sensitive data. That is, the SDT has endorsed permitting responsible entities to simply elect to plan and implement physical protections for communications links. This would “mitigate” the risk of an unauthorized disclosure or modification of data using one of the delineated methods. As such, the responsible entity would potentially be compliant with the standard without proposing or implementing any logical protections for sensitive data during its transmission. This appears counter to FERC’s intent to protect “both the integrity and availability of sensitive bulk electric system data.” FERC Order No. 822, P. 54. Texas RE maintains its recommendation to 1) change “or” to “and”; and 2) change the phrase risk of unauthorized disclosure or modification to integrity and availability of sensitive bulk electric system data.

Furthermore, Texas RE is also concerned with the SDT’s shortsighted approach to securing this type of data, which permits discretion around security matters that are not in controversy and are widely considered vulnerabilities that must be mitigated. This approach is also not consistent with the “defense in depth” philosophy, which is a fundamental aspect of cyber security domains. In other words, it is a more consistent with the defense in depth concept to mitigate the risk of unauthorized disclosure and modification for this data versus one without the other.

Additionally, since GO does not appear in the definition of Control Center, Texas RE suggests removing GO from the applicability section.

Likes 0	
Dislikes 0	
Response	

2. Requirement R1: The SDT modified Requirement R1 to state: "The Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) to mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring data while being transmitted between any applicable Control Centers. The Responsible Entity is not required to include oral communications in its plan." Do you agree with this revision? If not, please provide the basis for your disagreement and an alternate proposal.

Dennis Sismaet - Northern California Power Agency - 6

Answer	No
Document Name	

Comment

This is too prescriptive and unnecessary. IRO-010-2 R3.3 and TOP-003-3 R5.3 already provide reliability assurance requirements for RCs, BAs, GOs, GOPs, TOPs, TOs, and DPs. Additionally, NERC has a Standards Efficiency Initiative underway to get rid of standards and requirements such as CIP-012-1 and its' requirement 1.

Likes 0	
Dislikes 0	

Response

Marty Hostler - Northern California Power Agency - 5

Answer	No
Document Name	

Comment

This is too prescriptive and unnecessary. IRO-010-2 R3.3 and TOP-003-3 R5.3 already provide reliability assurance requirements for RCs, BAs, GOs, GOPs, TOPs, TOs, and DPs. Additionally, NERC has a Standards Efficiency Initiative underway to get rid of standards and requirements such as CIP-012-1 and its' requirement 1.

Likes 0	
Dislikes 0	

Response

Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman

Answer	No
Document Name	

Comment

Please refer to MRO NERC Standards Review Forum (NSRF) comments.

Likes 0	
Dislikes 0	

Response

Chris Gowder - Florida Municipal Power Agency - 3,4,5,6

Answer	No
Document Name	

Comment

: FMPA agrees with the below comments submitted by the NSRF:

The NSRF has the following three concerns and the double jeopardy of noncompliance with R1 and part 1.3.

Concern one (1); R1 states “The Responsible Entity shall implement …” where the Responsible Entity is noted within section 4.1, Functional Entities. So, each BA, GOP, GO, RC, TOP and TO shall implement a documented plan (s) to mitigate the risk of unauthorized disclosure or modification of Real-time Assessments and Real-time monitoring data. Part 1.3 states that “If the Control Centers are owned or operated by different Responsible Entities” which they will be (unless there is a vertically integrated Entity), those different Entities

already need to satisfy R1 since they are in section 4.1. This part 1.3 is redundant and is recommended to be removed.

Concern two (2); R1.3 states “… identify the responsibilities…” this identification of responsibilities is ambiguous as each Entity can only identify their own responsibilities to “mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring data…” per R1. In essence, just repeating the words within R1 is not enhancing system reliability by any means. Recommended to be removed for this concern.

Concern three (3) is similar to concern 1, where one Entity needs to identify the other Entity which will be a different entity (unless they are a vertically integrated Entity); those different Entities already need to satisfy R1 since they are in section 4.1. This part 1.3 is redundant and is recommended to be removed.

The NSRF recommends that part 1.3 be deleted in its entirety as all Functional Entities will be required to satisfy R1 and part 1.1 and 1.2.

The NSRF agrees with adding “except under CIP Exceptional Circumstances” in R1.

Likes 0	
Dislikes 0	

Response

Richard Montgomery - Florida Municipal Power Agency - 3,4,5,6

Answer	No
Document Name	

Comment
FMPA agrees with the below comments submitted by the NSRF: The NSRF has the following three concerns and the double jeopardy of noncompliance with R1 and part 1.3. Concern one (1); R1 states “The Responsible Entity shall implement …” where the Responsible Entity is noted within section 4.1, Functional Entities. So, each BA, GOP, GO, RC, TOP and TO shall implement a documented plan (s) to mitigate the risk of unauthorized disclosure or modification of Real-time Assessments and Real-time monitoring data. Part 1.3 states that “If the Control Centers are owned or operated by different Responsible Entities” which they will be (unless there is a vertically integrated Entity), those different Entities already need to satisfy R1 since they are in section 4.1. This part 1.3 is redundant and is recommended to be removed. Concern two (2); R1.3 states “… identify the responsibilities…” this identification of responsibilities is ambiguous as each Entity can only identify their own responsibilities to “mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring data…” per R1. In essence, just repeating the words within R1 is not enhancing system reliability by any means. Recommended to be removed for this concern. Concern three (3) is similar to concern 1, where one Entity needs to identify the other Entity which will be a different entity (unless they are a vertically integrated Entity); those different Entities already need to satisfy R1 since they are in section 4.1. This part 1.3 is redundant and is recommended to be removed. The NSRF recommends that part 1.3 be deleted in its entirety as all Functional Entities will be required to satisfy R1 and part 1.1 and 1.2. The NSRF agrees with adding “except under CIP Exceptional Circumstances” in R1.

Likes 0	
Dislikes 0	

Response

Brandon McCormick - Brandon McCormick On Behalf of: Ginny Beigel, City of Vero Beach, 3; Lynne Mila, City of Clewiston, 4; Mike Blough, Kissimmee Utility Authority, 5, 3; Tom Reedy, Florida Municipal Power Pool, 6; - Brandon McCormick, Group Name FMPA	
Answer	No
Document Name	

Comment
FMPA agrees with the below comments submitted by the NSRF: The NSRF has the following three concerns and the double jeopardy of noncompliance with R1 and part 1.3. Concern one (1); R1 states “The Responsible Entity shall implement …” where the Responsible Entity is noted within section 4.1, Functional Entities. So, each BA, GOP, GO, RC, TOP and TO shall implement a documented plan (s) to mitigate the risk of unauthorized disclosure or modification of Real-time Assessments and Real-time monitoring data. Part 1.3 states that “If the Control Centers are owned or operated by different Responsible Entities” which they will be (unless there is a vertically integrated Entity), those different Entities already need to satisfy R1 since they are in section 4.1. This part 1.3 is redundant and is recommended to be removed.

Concern two (2); R1.3 states "… identify the responsibilities…" this identification of responsibilities is ambiguous as each Entity can only identify their own responsibilities to "mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring data…" per R1. In essence, just repeating the words within R1 is not enhancing system reliability by any means. Recommended to be removed for this concern.

Concern three (3) is similar to concern 1, where one Entity needs to identify the other Entity which will be a different entity (unless they are a vertically integrated Entity); those different Entities already need to satisfy R1 since they are in section 4.1. This part 1.3 is redundant and is recommended to be removed.

The NSRF recommends that part 1.3 be deleted in its entirety as all Functional Entities will be required to satisfy R1 and part 1.1 and 1.2.

The NSRF agrees with adding "except under CIP Exceptional Circumstances" in R1

Likes 0	
Dislikes 0	

Response

Richard Jackson - U.S. Bureau of Reclamation - 1

Answer	No
Document Name	

Comment

It is not clear how a CIP Exceptional Circumstance would impact the mitigation of the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring data; therefore, Reclamation asserts that an exception for CIP Exceptional Circumstances is not necessary.

Likes 0	
Dislikes 0	

Response

Aaron Smith - Omaha Public Power District - 1,3,5,6

Answer	No
Document Name	

Comment

Comments: The NSRF has the following three concerns and the double jeopardy of noncompliance with R1 and part 1.3.

Concern one (1); R1 states "The Responsible Entity shall implement …" where the Responsible Entity is noted within section 4.1, Functional Entities. So, each BA, GOP, GO, RC, TOP and TO shall implement a documented plan (s) to mitigate the risk of unauthorized disclosure or modification of Real-time Assessments and Real-time monitoring data. Then in part 1.3 it states that "If the Control Centers are owned or operated by different Responsible Entities" which they will be (unless there is a vertically integrated Entity), those different Entities already need to satisfy R1 since they are in section 4.1. This part 1.3 is redundant and is recommended to be removed.

Concern two (2); R1.3 states "… identify the responsibilities…" this identification of responsibilities is ambiguous as each Entity can only identify their own responsibilities to "mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring data…" per R1. In essence, just repeating the words within R1 is not enhancing system reliability by any means. Recommended to be removed for this concern.

Concern three (3) is similar to concern 1, where one Entity needs to identify the other Entity which will be a different entity (unless they are a vertically integrated Entity); those different Entities already need to satisfy R1 since they are in section 4.1. This part 1.3 is redundant and is recommended to be removed.

The NSRF recommends that part 1.3 be deleted in its entirety as all Functional Entities will be required to satisfy R1 and part 1.1 and 1.2.

The NSRF agrees with adding "except under CIP Exceptional Circumstances" in R1.

Likes 0	
Dislikes 0	

Response

Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	No
Document Name	

Comment

The NSRF has the following three concerns and the double jeopardy of noncompliance with R1 and part 1.3.

Concern one (1); R1 states "The Responsible Entity shall implement …" where the Responsible Entity is noted within section 4.1, Functional Entities. So, each BA, GOP, GO, RC, TOP and TO shall implement a documented plan (s) to mitigate the risk of unauthorized disclosure or modification of Real-time Assessments and Real-time monitoring data. Part 1.3 states that "If the Control Centers are owned or operated by different Responsible Entities" which they will be (unless there is a vertically integrated Entity), those different Entities already need to satisfy R1 since they are in section 4.1. This part 1.3 is redundant and is recommended to be removed.

Concern two (2); R1.3 states "… identify the responsibilities…" this identification of responsibilities is ambiguous as each Entity can only identify their own responsibilities to "mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring data…" per R1. In essence, just repeating the words within R1 is not enhancing system reliability by any means. Recommended to be removed for this concern.

Concern three (3) is similar to concern 1, where one Entity needs to identify the other Entity which will be a different entity (unless they are a vertically integrated Entity); those different Entities already need to satisfy R1 since they are in section 4.1. This part 1.3 is redundant and is recommended to be removed.

The NSRF recommends that part 1.3 be deleted in its entirety as all Functional Entities will be required to satisfy R1 and part 1.1 and 1.2.

The NSRF agrees with adding "except under CIP Exceptional Circumstances" in R1.

Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - MRO, Group Name SPP Standards Review Group	
Answer	Yes
Document Name	
Comment	
The SPP Standards Review Group has no issues with the language proposed, however, we would recommend that the SDT include an example pertaining to the under CIP Exceptional Circumstances in the Implementation Guidance Document.	
Likes 0	
Dislikes 0	
Response	
David Francis - Midcontinent ISO, Inc. - 2 - MRO,SERC,RF	
Answer	Yes
Document Name	
Comment	
Adding that statement clarifies the excludes meaning	
Likes 0	
Dislikes 0	
Response	
Warren Cross - ACES Power Marketing - 1,3,4,5 - MRO,WECC,Texas RE,SERC	
Answer	Yes
Document Name	
Comment	
ACES supports the modified R1.	
Likes 0	
Dislikes 0	

Response
Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran
Answer	Yes
Document Name	
Comment
Oncor supports EEI's comment.
Likes 0	
Dislikes 0	
Response
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company
Answer	Yes
Document Name	
Comment
Southern Company supports the proposed revisions.
Likes 0	
Dislikes 0	
Response
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC
Answer	Yes
Document Name	
Comment
None
Likes 0	
Dislikes 0	
Response

Andrea Koch - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI supports the Requirement 1 revisions. EEI also supports the flexibility provided by Requirement 1; however, there are many different approaches to mitigating the risk of unauthorized disclosure or modification of data in transit. Additional guidance that explores various approaches and evaluates their effectiveness in mitigating risk may be helpful before entities make implementation investments for CIP-012-1.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion	
Answer	Yes
Document Name	
Comment	
Is <<Real-time monitoring data>> the same as operational data? Operational data is in other Standards	
Likes 0	
Dislikes 0	
Response	
Eli Rivera - Central Electric Cooperative, Inc. (Redmond, Oregon) - NA - Not Applicable - Texas RE	
Answer	Yes
Document Name	
Comment	
CenterPoint Energy Houston Electric, LLC (“CenterPoint Energy”) agrees with Edison Electric Institute’s (EEI) comments.	
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 agrees with the proposed revision.	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon supports the Requirement 1 revisions. Exelon also supports the flexibility provided by Requirement 1; however, there are many different approaches to mitigating the risk of unauthorized disclosure or modification of data in transit. Additional guidance that explores various approaches and evaluates their effectiveness in mitigating risk may be helpful before entities make implementation investments for CIP-012-1.	
Likes 0	
Dislikes 0	
Response	
Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	Yes
Document Name	
Comment	
NRECA supports the modified R1; however, we request that the SDT provide clarification on why R1.3 is needed, especially when R1, R1.1 and R1.2 seem to have an overlap in what is required with R1.3. With a clarification on the need for R1.3, NRECA believes that will help registered entities to better understand why R1.3 is necessary. With this clarification, it may not be necessary to remove R1.3.	
Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	

Answer	Yes
Document Name	
Comment	

NV Energy agrees with the requirement based on the newly introduced paragraph in the Implementation Guidance, “Where the operational obligations of an entire communication link, including both endpoints, belong to the Control Center of another Responsible Entity, the Responsible Entity without operational obligations for the communication link may demonstrate compliance by ensuring the communications link endpoint is within its Control Center, which could be limited to including the communication link endpoint within a PSP.”

NV Energy would like the following edit added “or where other physical protections are applied.” NV Energy believes that this will allow entities flexibility where their devices that perform this function are located within its location. NV Energy believes the VPN examples provided are necessary and should remain within the Guidance document. If the newly introduced paragraph or the VPN example are removed or if the implementation guidance is not ERO-endorsed prior to the final ballot, NV Energy may alter its final vote.

Likes 0	
Dislikes 0	
Response	

Darnez Gresham - Darnez Gresham On Behalf of: Annette Johnston, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Darnez Gresham

Answer	Yes
Document Name	
Comment	

MEC agrees with the requirement based on the newly introduced sentence in the Implementation Guidance, “Where the operational obligations of an entire communication link, including both endpoints, belong to the Control Center of another Responsible Entity, the Responsible Entity without operational obligations for the communication link may demonstrate compliance by ensuring the communications link endpoint is within its Control Center, which could be limited to including the communication link endpoint within a PSP.” MEC would like the following edit added “or where other physical protections are applied.” This will provide more flexibility for entities. MEC also likes the VPN example provided. Inclusion of the newly introduced sentence, the VPN example and ERO-endorsement of the implementation guidance are needed in the final version for MEC to vote yes on the final ballot.

Likes 0	
Dislikes 0	
Response	

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6

Answer	Yes
Document Name	
Comment	

PacifiCorp agrees with the requirement based on the newly introduced paragraph in the Implementation Guidance, “Where the operational obligations of an entire communication link, including both endpoints, belong to the Control Center of another Responsible Entity, the Responsible Entity without operational obligations for the communication link may demonstrate compliance by ensuring the communications link endpoint is within its Control Center, which could be limited to including the communication link endpoint within a PSP.” PacifiCorp would like the following edit added “or where other physical protections are applied.” PacifiCorp feels that this will allow entities flexibility where the devices that perform this are located within its location. PacifiCorp also likes the VPN examples provided. If the newly introduced paragraph or the VPN example are removed or if the implementation guidance is not ERO-endorsed prior to the final ballot, PacifiCorp may alter its final vote.

Likes 0	
Dislikes 0	

Response

Laura Nelson - IDACORP - Idaho Power Company - 1

Answer	Yes
Document Name	

Comment

It is always good to include exceptions for unforeseen circumstances and emergencies.

Likes 0	
Dislikes 0	

Response

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI

Answer	Yes
Document Name	

Comment

AECI and members of the AECI group are supportive of the comments provided by NRECA.

Likes 0	
Dislikes 0	

Response

Russell Martin II - Salt River Project - 1,3,5,6 - WECC

Answer	Yes
Document Name	

Comment
SRP agrees the data should be protected. SRP also agrees the protections for the data in scope must ensure the data has not been modified, and that FERC directed NERC to “specify how the confidentiality, integrity, and availability of each type of bulk electric system data should be protected while it is being transmitted.” However, SRP takes exception to the extent the proposed standard requires the data in scope to be protected. FERC Order 822 states on page 36, “…we recognize that not all communication network components and data pose the same risk to bulk electric system reliability and may not require the same level of protection.” However, the proposed standard applies the same criteria of protection against unauthorized disclosure across all of the data within the defined scope. SRP does not agree viewing of the Real-time Assessment and Real-time monitoring and control data without context will decrease the reliable operation of the BES and asserts confidentiality does not need to be protected for all data under this scope. Along with this, SRP would like a clarification of how the SDT defines Real-Time Assessment Data. Additionally, SRP recognizes the SDT is not specifying the controls used to protect confidentiality and integrity. However, the only method available to achieve the proposed required objective is to implement encryption. FERC Order 822 states on page 39, “it is reasonable to conclude that any lag in communication speed resulting from implementation of protections [encryption technologies] should only be measureable on the order of milliseconds and, therefore, will not adversely impact Control Center communications,” but SRP asserts this statement only refers to a single data stream. It is unknown what encryption will do when dealing with multiple data streams being transmitted at once, from one to many points, not only to the latency added for the reliable operation of the BES, but also to the computing resources

Likes 0	
Dislikes 0	

Response

Teresa Cantwell - Lower Colorado River Authority - 1,5	
Answer	Yes
Document Name	

Comment
None

Likes 0	
Dislikes 0	

Response

Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 3	
Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response	
Quintin Lee - Eversource Energy - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Greyerbiehl - CMS Energy - Consumers Energy Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Wagner - Santee Cooper - 1, Group Name Santee Cooper	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
James Anderson - CMS Energy - Consumers Energy Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Douglas Johnson - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Stephanie Burns - Stephanie Burns On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Stephanie Burns	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Jeff Johnson - Jeff Johnson On Behalf of: Martine Blair, Sempra - San Diego Gas and Electric, 3, 5, 1; - Jeff Johnson	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Douglas Webb - Douglas Webb On Behalf of: Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; James McBee, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; Jessica Tucker, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; Jim Flucke, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; Megan Wagner, Westar Energy, 6, 3, 1, 5; - Douglas Webb	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response
Michael Shaw - Lower Colorado River Authority - 1

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Ramkalawan - Ontario Power Generation Inc. - 5	
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	
Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 1,3,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 3, Group Name FirstEnergy Corporation	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aubrey Short - FirstEnergy - FirstEnergy Corporation - 4	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Maier - Intermountain REA - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thomas Foltz - AEP - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steve Rose - City Water, Light and Power of Springfield, IL - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE does not have comments on this question.	
Likes 0	
Dislikes 0	

Response

Joe McKinney - Florida Municipal Power Agency - 3,4,5,6	
Answer	
Document Name	
Comment	

: FMPA agrees with the below comments submitted by the NSRF:

The NSRF has the following three concerns and the double jeopardy of noncompliance with R1 and part 1.3.

Concern one (1); R1 states “The Responsible Entity shall implement …” where the Responsible Entity is noted within section 4.1, Functional Entities. So, each BA, GOP, GO, RC, TOP and TO shall implement a documented plan (s) to mitigate the risk of unauthorized disclosure or modification of Real-time Assessments and Real-time monitoring data. Part 1.3 states that “If the Control Centers are owned or operated by different Responsible Entities” which they will be (unless there is a vertically integrated Entity), those different Entities

already need to satisfy R1 since they are in section 4.1. This part 1.3 is redundant and is recommended to be removed.

Concern two (2); R1.3 states “… identify the responsibilities…” this identification of responsibilities is ambiguous as each Entity can only identify their own responsibilities to “mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring data…” per R1. In essence, just repeating the words within R1 is not enhancing system reliability by any means. Recommended to be removed for this concern.

Concern three (3) is similar to concern 1, where one Entity needs to identify the other Entity which will be a different entity (unless they are a vertically integrated Entity); those different Entities already need to satisfy R1 since they are in section 4.1. This part 1.3 is redundant and is recommended to be removed.

The NSRF recommends that part 1.3 be deleted in its entirety as all Functional Entities will be required to satisfy R1 and part 1.1 and 1.2.

The NSRF agrees with adding “except under CIP Exceptional Circumstances” in R1.

Likes 0	

Dislikes 0	

Response

Carol Chinn - Florida Municipal Power Agency - 3,4,5,6	
Answer	
Document Name	

Comment
: FMPA agrees with the below comments submitted by the NSRF: The NSRF has the following three concerns and the double jeopardy of noncompliance with R1 and part 1.3. Concern one (1); R1 states “The Responsible Entity shall implement …” where the Responsible Entity is noted within section 4.1, Functional Entities. So, each BA, GOP, GO, RC, TOP and TO shall implement a documented plan (s) to mitigate the risk of unauthorized disclosure or modification of Real-time Assessments and Real-time monitoring data. Part 1.3 states that “If the Control Centers are owned or operated by different Responsible Entities” which they will be (unless there is a vertically integrated Entity), those different Entities already need to satisfy R1 since they are in section 4.1. This part 1.3 is redundant and is recommended to be removed. Concern two (2); R1.3 states “… identify the responsibilities…” this identification of responsibilities is ambiguous as each Entity can only identify their own responsibilities to “mitigate the risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring data…” per R1. In essence, just repeating the words within R1 is not enhancing system reliability by any means. Recommended to be removed for this concern. Concern three (3) is similar to concern 1, where one Entity needs to identify the other Entity which will be a different entity (unless they are a vertically integrated Entity); those different Entities already need to satisfy R1 since they are in section 4.1. This part 1.3 is redundant and is recommended to be removed. The NSRF recommends that part 1.3 be deleted in its entirety as all Functional Entities will be required to satisfy R1 and part 1.1 and 1.2. The NSRF agrees with adding “except under CIP Exceptional Circumstances” in R1.

Likes 0	
Dislikes 0	

Response

3. Implementation Plan: The SDT established the Implementation Plan to make the standard effective the first day of the first calendar quarter that is twenty-four (24) calendar months after the effective date of the applicable governmental authority's order approving the standard, or as otherwise provided for by the applicable governmental authority. Do you agree with this proposal? If you think an alternate implementation time period is needed, please provide a detailed explanation of actions and time needed to meet the implementation deadline.

Russell Martin II - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	

Overall, SRP does not agree with twenty-four (24) calendar months for the implementation of Requirements R1, as R1 and R2 from the second draft have been merged. Although SRP recognizes the SDT is not specifying the controls to be used to protect confidentiality and integrity, the only examples provided in the implementation guidance includes encryption. If there are other methods available to achieve the security objective, SRP asks the SDT to provide them. However, the only method available to achieve the proposed required objective, on the ICCP network, is to implement encryption. As FERC order 822 states on page 37, "if several registered entities have joint responsibility for a cryptographic key management system used between their respective Control Centers, they should have the prerogative to come to a consensus on which organization administers that particular key management system." Furthermore, the FERC order states on page 38, "While responsible entities are required to exchange real-time and operational planning data necessary to operate the bulk electric system using mutually agreeable security protocols, there is no technical specification for how this transfer of information should incorporate mandatory security controls." These are activities and specifications that must be created and agreed upon by all registered entities involved in the data transfer. As such the timeline is reliant on registered entities working together on a common solution and would not be achievable within 24 calendar months.

Additionally, if encryption fails, SRP would lose Real-time Assessment and Real-time monitoring and control data. There are many opportunities for encryption to fail that must be addressed. The implementation of encryption requires a pilot to truly understand and address the mechanisms of failure, the impacts encryption would cause on the exchange of the data, and the computing resources required. A pilot also requires a great amount of coordination to execute, not only within the industry, but may also include carriers, vendors, and possibly third-party encryption key program managers.

Because of the aforementioned reasons and concerns, SRP is recommending a phased implementation for CIP-012-1. A 24 month implementation is appropriate, but only for Requirement R1. The 24 months for R1 would provide time to coordinate and create an industry-wide solution. SRP is proposing the SDT include an additional 12 months for the plan implementation aspect of Requirement R1. The additional 12 months would be used for a pilot and course correction if needed, in addition to understanding, formulating, and executing maintenance strategies.

Likes 0	
Dislikes 0	

Response

Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	No
Document Name	
Comment	

WECC believes the Implementation Plan of 24 months is unnecessary and the standard 18-month Implementation Plan should suffice. However, if the clarification sought in question 1 above is provided, WECC would not vote NO solely based on the length of the Implementation Plan.

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

Duke Energy disagrees that twenty-four calendar (24) months is enough time for implementation. We reiterate our previous comment and suggest a staggered implementation plan for CIP-012 specifically concerning coordination with neighboring entities. We consider it possible for an entity to gather necessary data, convening of internal work groups, and drafting of security protection plans in the proposed 24 month Implementation Plan. However, we feel that the coordination with other entities that will be necessary for R1.3 will take longer than the proposed 24 months, especially with internal work already taking place. We recommend the drafting team consider a staggered implementation plan for internal work (18 months) compared to external coordination work (36 months). When considering coordination/testing with neighboring entities, possible equipment upgrades/lead times that could ensue, we feel that additional time above the proposed 24-month Implementation Plan is warranted.

Likes 0	
Dislikes 0	

Response

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

BPA agrees with the intent of the FERC Directive. BPA is concerned about the proposed solution and its implementation timeline.

BPA requests that the SDT incorporate a pilot project to validate the proposed solution; is designed to address the FERC directive. Additionally, BPA requests the implementation timeframe to be extended to a 36 month phased implementation timeline; to begin upon successful completion of the pilot project. The industry needs 36 months due to the large amount of applicable data, access to funds, budget cycle, and resources to perform work required.

BPA is concerned about 3rd party encryption keys and the risks they pose, including the expiration of encryption keys. When an encryption key expires, the data flow ceases immediately to include Real-time Assessment and Real-time monitoring and control data. BPA requests that controls be put in place to ensure mitigation measures do not allow encryption keys to expire. Additionally, BPA is concerned that there is a risk of the certificate authority

being unavailable for authentication, impacting maintenance of reliable communications between control centers for operation of the Bulk Electric System.

BPA also agrees with SRP comments, as follows:

“Overall, SRP does not agree with twenty-four (24) calendar months for the implementation of Requirements R1, as R1 and R2 from the second draft have been merged. Although SRP recognizes the SDT is not specifying the controls to be used to protect confidentiality and integrity, the only examples provided in the implementation guidance includes encryption. If there are other methods available to achieve the security objective, SRP asks the SDT to provide them. However, the only method available to achieve the proposed required objective, on the ICCP network, is to implement encryption. As FERC order 822 states on page 37, “if several registered entities have joint responsibility for a cryptographic key management system used between their respective Control Centers, they should have the prerogative to come to a consensus on which organization administers that particular key management system.” Furthermore, the FERC order states on page 38, “While responsible entities are required to exchange real-time and operational planning data necessary to operate the bulk electric system using mutually agreeable security protocols, there is no technical specification for how this transfer of information should incorporate mandatory security controls.” These are activities and specifications that must be created and agreed upon by all registered entities involved in the data transfer. As such the timeline is reliant on registered entities working together on a common solution and would not be achievable within 24 calendar months.

Additionally, if encryption fails, SRP would lose Real-time Assessment and Real-time monitoring and control data. There are many opportunities for encryption to fail that must be addressed. The implementation of encryption requires a pilot to truly understand and address the mechanisms of failure, the impacts encryption would cause on the exchange of the data, and the computing resources required. A pilot also requires a great amount of coordination to execute, not only within the industry, but may also include carriers, vendors, and possibly third-party encryption key program managers.

Because of the aforementioned reasons and concerns, SRP is recommending a phased implementation for CIP-012-1. A 24 month implementation is appropriate, but only for Requirement R1. The 24 months for R1 would provide time to coordinate and create an industry-wide solution. SRP is proposing the SDT include an additional 12 months for the plan implementation aspect of Requirement R1. The additional 12 months would be used for a pilot and course correction if needed, in addition to understanding, formulating, and executing maintenance strategies.”

Likes 0	
Dislikes 0	

Response

Marty Hostler - Northern California Power Agency - 5

Answer	No
Document Name	

Comment

No, this standard should never be implemented! This is too prescriptive and unnecessary. IRO-010-2 R3.3 and TOP-003-3 R5.3 already provide reliability assurance requirements for RCs, BAs, GOs, GOPs, TOPs, TOs, and DPs. Additionally, NERC has a Standards Efficiency Initiative underway to get rid of standards and requirements such as CIP-012-1 and its' requirement 1.

Likes 0	
Dislikes 0	

Response

Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	
Comment	
No, this standard should never be implemented! This is too prescriptive and unnecessary. IRO-010-2 Question 3	
Likes 0	
Dislikes 0	
Response	
Joe McKinney - Florida Municipal Power Agency - 3,4,5,6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Gowder - Florida Municipal Power Agency - 3,4,5,6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5	
Answer	Yes
Document Name	
Comment	

None	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
The implementation plan is agreeable for a new CIP requirement to provide ample time to evaluate the impact and prepare the appropriate controls and procedures.	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 1,3,6	
Answer	Yes
Document Name	
Comment	
Ameren supports the proposed twenty-four (24) month implementation plan due to the complexity of securing control center to control center communications, which will require significant external coordination, procurement and installation of new technology and processes, legal reviews, and training. Technical challenges to implementing the standard will also be significant. For example, entities may deploy Secure ICCP as their CIP-012-1 solution. The Pacific Northwest National Laboratory's ("PNNL") June 2017 report, "Secure ICCP," identifies technical and other challenges for entities implementing secure ICCP (e.g., limited industry experience, documentation, support, difficulties with software upgrades and patching). The PNNL report is available at: https://www.pnnl.gov/main/publications/external/technical_reports/PNNL-26729.pdf. While these issues are not insurmountable they will take time, and should not be inappropriately rushed.	
Likes 0	
Dislikes 0	
Response	

Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
With any Standard that provides multiple iterations for proving compliance, a longer timeline is necessary, and we support a 24 month window for implementation.	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon supports the proposed twenty-four (24) month implementation plan due to the complexity of securing control center to control center communications, which will require significant external coordination, procurement and installation of new technology and processes, legal reviews, and training.	
Likes 0	
Dislikes 0	
Response	

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion	
Answer	Yes
Document Name	
Comment	
Considering the complexity, it is estimated that 36 calendar months would be required to comply.	
Likes 0	
Dislikes 0	
Response	
Andrea Koch - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI supports the proposed twenty-four (24) month implementation plan due to the complexity of securing control center to control center communications, which will require significant external coordination, procurement and installation of new technology and processes, legal reviews, and training. Technical challenges to implementing the standard will also be significant. For example, entities may deploy Secure ICCP as their CIP-012-1 solution. The Pacific Northwest National Laboratory's ("PNNL") June 2017 report, "Secure ICCP," identifies technical and other challenges for entities implementing secure ICCP (e.g., limited industry experience, documentation, limited user community, support, difficulties with software upgrades and patching). The report details the implementation of Secure ICCP using the same EMS vendor software. Similar installations using different or comingled EMS vendor software may prove to be even more challenging. The PNNL report is available at: https://www.pnnl.gov/main/publications/external/technical_reports/PNNL-26729.pdf. In order to ensure there is sufficient time to address such reliability and compliance issues, EEI supports NERC's proposed twenty-four (24) month implementation plan.	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	

Southern Company supports the proposed twenty-four (24) month implementation plan.	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran	
Answer	Yes
Document Name	
Comment	
Oncor supports EEI's comment.	
Likes 0	
Dislikes 0	
Response	
Warren Cross - ACES Power Marketing - 1,3,4,5 - MRO,WECC,Texas RE,SERC	
Answer	Yes
Document Name	
Comment	
:ACES believes that twenty-four (24) calendar months after the effective date of the applicable governmental authority's order approving the standard for implementation is appropriate.	
Likes 0	
Dislikes 0	
Response	
David Francis - Midcontinent ISO, Inc. - 2 - MRO,SERC,RF	
Answer	Yes
Document Name	
Comment	

However, because this may invovle third parites equiement being place or added to a PSP based on the Technical Rationale and Justification for Reliability Standard guidance may need extended design and implementation efforts in meeting the PSP security requirments

Likes 0	
Dislikes 0	

Response

Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 3

Answer	Yes
Document Name	

Comment

While it will take less time for entities to implement intra-entity solutions, it will take time for inter-entity solutions to be drafted and agreed upon. Since both entities will need to agree on not just implementing a technical solution (e.g. IPSec, Secure ICCP), but how to maintain it (e.g. cryptography key management).

Likes 0	
Dislikes 0	

Response

Steve Rose - City Water, Light and Power of Springfield, IL - 1,3,5

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Thomas Foltz - AEP - 5

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	
Response	
David Maier - Intermountain REA - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aubrey Short - FirstEnergy - FirstEnergy Corporation - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 3, Group Name FirstEnergy Corporation	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Smith - Omaha Public Power District - 1,3,5,6	
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	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Shaw - Lower Colorado River Authority - 1	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brandon McCormick - Brandon McCormick On Behalf of: Ginny Beigel, City of Vero Beach, 3; Lynne Mila, City of Clewiston, 4; Mike Blough, Kissimmee Utility Authority, 5, 3; Tom Reedy, Florida Municipal Power Pool, 6; - Brandon McCormick, Group Name FMPA	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb On Behalf of: Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; James McBee, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; Jessica Tucker, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; Jim Flucke, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; Megan Wagner, Westar Energy, 6, 3, 1, 5; - Douglas Webb	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Richard Montgomery - Florida Municipal Power Agency - 3,4,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Carol Chinn - Florida Municipal Power Agency - 3,4,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Darnez Gresham On Behalf of: Annette Johnston, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Darnez Gresham	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jeff Johnson - Jeff Johnson On Behalf of: Martine Blair, Sempra - San Diego Gas and Electric, 3, 5, 1; - Jeff Johnson	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Stephanie Burns - Stephanie Burns On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Stephanie Burns	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eli Rivera - Central Electric Cooperative, Inc. (Redmond, Oregon) - NA - Not Applicable - Texas RE	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Douglas Johnson - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Anderson - CMS Energy - Consumers Energy Company - 1	
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	
Martin Sidor - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Greyerbiehl - CMS Energy - Consumers Energy Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - MRO, Group Name SPP Standards Review Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

4. Technical Rationale: The SDT modified the draft Technical Rationale for CIP-012 to further explain the need for the exemption for certain Control Centers. Do you agree with the explanations and included diagrams in the draft Technical Rationale? If you do not agree, or if you agree but have comments or suggestions for the draft Technical Rationale, please provide your recommendation and explanation.

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - MRO, Group Name SPP Standards Review Group

Answer	No
Document Name	

Comment

The SPP Standards Review Group has a concern that the proposed Exemption will modify the current “Control Center” definition that potentially changes how High and Low impacts assets are evaluated. The review group is proposing some language (shown below) to help maintain consistency with the “Control Center” Definition and the proposed Exemption mentioned in the documentation. Additionally, the introduction of the term “Control System” as well as the diagrams and explanations in the rationale present complexity pertaining to the current process of identifying BES Cyber Systems. We would suggest that the drafting team remove the term “Control System” from all proposed language associated with this project.

Section 4.2.3. (Applicability Section –Standard)

A **BES** generation resource or Transmission station or substation that transmits to a Control Center Real-time Assessment or Real-time monitoring data**, such as RTU-style data,** pertaining only to the generation resource or Transmission station or substation at which the **data transmitted** is located.

Likes 0	
Dislikes 0	

Response

David Francis - Midcontinent ISO, Inc. - 2 - MRO,SERC,RF

Answer	No
Document Name	

Comment

Increases security risk with repair personnel going into a PSP without knowning all the CIP security requirments for such devises and have in house personnel escorting the repair personnel during any repair work

Likes 0	
Dislikes 0	

Response

David Greyerbiehl - CMS Energy - Consumers Energy Company - 5

Answer	No

Document Name	
Comment	
In the Technical Rationale document, please specify what type of date under TOP-003 and IRO-010 should be excluded from the CIP-012 requirements.	
Likes 0	
Dislikes 0	
Response	
James Anderson - CMS Energy - Consumers Energy Company - 1	
Answer	No
Document Name	
Comment	
In the Technical Rationale document, please specify what type of date under TOP-003 and IRO-010 should be excluded from the CIP-012 requirements.	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	No
Document Name	
Comment	
Please refer to MRO NERC Standards Review Forum (NSRF) comments.	
Likes 0	
Dislikes 0	
Response	
Stephanie Burns - Stephanie Burns On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Stephanie Burns	
Answer	No

Document Name	

Comment

The technical rational should show examples of demarcation points for the protections or define the demarcation points. For example, if a leased line or router is not owned by the entity, however the entity chose to deploy a firewall to encrypt the traffic ahead of the router, then the firewall shall be the demarcation point, not the router. Explanations left to the entity without proper guidance may lead to confusion. Furthermore, while entities may not own both sides of the links, technologies such as VPN require both sides to follow the same configuration in order to encrypt data. If the other side is not equipped to encrypt the data, the link will remain unsecure.

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

Duke Energy suggests the drafting team consider adding a diagram that demonstrates under what circumstances a generating resource or Transmission sub would be applicable to this standard. With the added exemption language, it would be helpful for the industry to have a couple of examples where the exemption would not apply to existing generation resources and Transmission subs.

Likes 0	
Dislikes 0	

Response

Chris Gowder - Florida Municipal Power Agency - 3,4,5,6

Answer	No
Document Name	

Comment

FMPA agrees with the following comments submitted by the NSRF:

The NSRF does not agree that Figure 2 and related discussion within the Technical Rationale document applies to Transmission stations and substations and generation resources as being “Control Centers”. The NSRF believes that the Control Center definition was developed with the intent to apply to functionally manned control centers that monitor and control the BES; a center that hosts System Operators that have specific training requirements and in some instances certifications to meet the requirements of their position. It appears the drafting team is expanding the Control Center definition for a field asset application in order to meet the needs of an exemption for CIP-012. Consider also, that in the last sentence of the first paragraph of the Reference Model Discussion in the Implementation Guidance it correctly states “Additionally, Entity Alpha does not need to consider any communications to other non-Control Center facilities such as generating plants or substations. These communications are out of scope for CIP-012-1” [emphasis added] The NSRF does agree that RTU-style data transmission between BES generation and Transmission stations and substations

need to be explicitly excluded from CIP-012. The NSRF, under Comment #1 on this form, has provided revision language that meets our comments here and those already addressed

Likes 0	
Dislikes 0	

Response

Joe McKinney - Florida Municipal Power Agency - 3,4,5,6

Answer	No
Document Name	

Comment

FMPA agrees with the following comments submitted by the NSRF:

The NSRF does not agree that Figure 2 and related discussion within the Technical Rationale document applies to Transmission stations and substations and generation resources as being “Control Centers”. The NSRF believes that the Control Center definition was developed with the intent to apply to functionally manned control centers that monitor and control the BES; a center that hosts System Operators that have specific training requirements and in some instances certifications to meet the requirements of their position. It appears the drafting team is expanding the Control Center definition for a field asset application in order to meet the needs of an exemption for CIP-012. Consider also, that in the last sentence of the first paragraph of the Reference Model Discussion in the Implementation Guidance it correctly states “Additionally, Entity Alpha does not need to consider any communications to other non-Control Center facilities such as generating plants or substations. These communications are out of scope for CIP-012-1” [emphasis added].

Likes 0	
Dislikes 0	

Response

Carol Chinn - Florida Municipal Power Agency - 3,4,5,6

Answer	No
Document Name	

Comment

FMPA agrees with the following comments submitted by the NSRF:

The NSRF does not agree that Figure 2 and related discussion within the Technical Rationale document applies to Transmission stations and substations and generation resources as being “Control Centers”. The NSRF believes that the Control Center definition was developed with the intent to apply to functionally manned control centers that monitor and control the BES; a center that hosts System Operators that have specific training requirements and in some instances certifications to meet the requirements of their position. It appears the drafting team is expanding the Control Center definition for a field asset application in order to meet the needs of an exemption for CIP-012. Consider also, that in the last sentence of the first paragraph of the Reference Model Discussion in the Implementation Guidance it correctly states “Additionally, Entity Alpha does not need to consider

any communications to other non-Control Center facilities such as generating plants or substations. These communications are out of scope for CIP-012-1" [emphasis added].

Likes 0	
Dislikes 0	

Response

Richard Montgomery - Florida Municipal Power Agency - 3,4,5,6

Answer	No
Document Name	

Comment

FMPA agrees with the following comments submitted by the NSRF:

The NSRF does not agree that Figure 2 and related discussion within the Technical Rationale document applies to Transmission stations and substations and generation resources as being "Control Centers". The NSRF believes that the Control Center definition was developed with the intent to apply to functionally manned control centers that monitor and control the BES; a center that hosts System Operators that have specific training requirements and in some instances certifications to meet the requirements of their position. It appears the drafting team is expanding the Control Center definition for a field asset application in order to meet the needs of an exemption for CIP-012. Consider also, that in the last sentence of the first paragraph of the Reference Model Discussion in the Implementation Guidance it correctly states "Additionally, Entity Alpha does not need to consider any communications to other non-Control Center facilities such as generating plants or substations. These communications are out of scope for CIP-012-1" [emphasis added].

Likes 0	
Dislikes 0	

Response

Brandon McCormick - Brandon McCormick On Behalf of: Ginny Beigel, City of Vero Beach, 3; Lynne Mila, City of Clewiston, 4; Mike Blough, Kissimmee Utility Authority, 5, 3; Tom Reedy, Florida Municipal Power Pool, 6; - Brandon McCormick, Group Name FMPA

Answer	No
Document Name	

Comment

Comments: FMPA agrees with the following comments submitted by the NSRF:

The NSRF does not agree that Figure 2 and related discussion within the Technical Rationale document applies to Transmission stations and substations and generation resources as being "Control Centers". The NSRF believes that the Control Center definition was developed with the intent to apply to functionally manned control centers that monitor and control the BES; a center that hosts System Operators that have specific training requirements and in some instances certifications to meet the requirements of their position. It appears the drafting team is expanding the Control Center definition for a field asset application in order to meet the needs of an exemption for CIP-012. Consider also, that in the last sentence of the first paragraph of the Reference Model Discussion in the Implementation Guidance it correctly states "Additionally, Entity Alpha does not need to consider

any communications to other non-Control Center facilities such as generating plants or substations. These communications are out of scope for CIP-012-1" [emphasis added].

The NSRF does agree that RTU-style data transmission between BES generation and Transmission stations and substations need to be explicitly excluded from CIP-012. The NSRF, under Comment #1 on this form, has provided revision language that meets our comments here and those already addressed

Likes 0	
Dislikes 0	

Response

Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,4,5 - RF

Answer	No
Document Name	

Comment

In the Technical Rationale document, please specify what type of date under TOP-003 and IRO-010 should be excluded from the CIP-012 requirements.

Likes 0	
Dislikes 0	

Response

Richard Jackson - U.S. Bureau of Reclamation - 1

Answer	No
Document Name	

Comment

Reclamation recommends that all Real-time Assessment and Real-time monitoring data be protected against the risk of unauthorized disclosure or modification. Reclamation asserts that the need to protect the data from a GOP Control Center with the ability to control more than two geographically separated facilities is no different than the need to protect the data from each single location, and no different from the need to protect data from a GOP Control Center to an RC or BA Control Center.

Likes 0	
Dislikes 0	

Response

Aaron Smith - Omaha Public Power District - 1,3,5,6

Answer	No
Document Name	

Comment

The NSRF does not agree that Figure 2 and related discussion within the Technical Rationale document applies to Transmission stations and substations and generation resources as being “Control Centers”. The NSRF believes that the Control Center definition was developed with the intent to apply to functionally manned control centers that monitor and control the BES; a center that hosts System Operators that have specific training requirements and in some instances certifications to meet the requirements of their position. It appears the drafting team is expanding the Control Center definition for a field asset application in order to meet the needs of an exemption for CIP-012. Consider also, that in the last sentence of the first paragraph of the Reference Model Discussion in the Implementation Guidance it correctly states “Additionally, Entity Alpha does not need to consider any communications to other non-Control Center facilities such as generating plants or substations. These communications are out of scope for CIP-012-1” [emphasis added].

The NSRF does agree that RTU-style data transmission between BES generation and Transmission stations and substations need to be explicitly excluded from CIP-012. The NSRF, under Comment #1 on this form, has provided revision language that meets our comments here and those already addressed.

Likes 0	
Dislikes 0	

Response

David Jendras - Ameren - Ameren Services - 1,3,6

Answer	No
Document Name	

Comment

We believe that any of the technical rationale that can be condensed into clear, concise language should be moved into the CIP-012-1 as a defined requirement. Responsible Entities are audited to the Requirements in the Standard. Leaving this much information as Technical Rationale invites subjective audit interpretation unnecessarily increases compliance risk for the entity.

Likes 0	
Dislikes 0	

Response

Laura Nelson - IDACORP - Idaho Power Company - 1

Answer	No
Document Name	

Comment

Idaho Power believes Figures 2 & 3 start to muddy the waters a little bit in terms of the initial intent of the CIP-012. Figure 2 seems to state that Station Alpha would be considered a control center, but Figure 3 seems to state that the communication between Station Alpha and the TOP control center would not be in scope of CIP-012. While Idaho Power would agree that in the end that seems to get to of the objective of the initial intent of CIP-012, this seems like a confusing way to reach that conclusion.

Likes 0	
Dislikes 0	

Response

Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	No
Document Name	

Comment

The NSRF does not agree that Figure 2 and related discussion within the Technical Rationale document applies to Transmission stations and substations and generation resources as being “Control Centers”. The NSRF believes that the Control Center definition was developed with the intent to apply to functionally manned control centers that monitor and control the BES; a center that hosts System Operators that have specific training requirements and in some instances certifications to meet the requirements of their position. It appears the drafting team is expanding the Control Center definition for a field asset application in order to meet the needs of an exemption for CIP-012. Consider also, that in the last sentence of the first paragraph of the Reference Model Discussion in the Implementation Guidance it correctly states “Additionally, Entity Alpha does not need to consider any communications to other non-Control Center facilities such as generating plants or substations. These communications are out of scope for CIP-012-1” [emphasis added].

The NSRF does agree that RTU-style data transmission between BES generation and Transmission stations and substations need to be explicitly excluded from CIP-012. The NSRF, under Comment #1 on this form, has provided revision language that meets our comments here and those already addressed.

Likes 0	
Dislikes 0	

Response

Thomas Foltz - AEP - 5

Answer	No
Document Name	

Comment

AEP requests the SDT consider including some statements in the Technical Rationale to address the possibility that data requests made related to TOP-003 and/or IRO-010 include other data that is not Real-time Assessment data or Real-time monitoring data, and how the Responsible Entity could exclude this other data from the security requirements.

The following text on page vi may need to be edited for sake of clarity “The only thing that has changed is an HMI for Station Beta has been moved within close physical proximity to an HMI for Station Alpha.”	
Likes 0	
Dislikes 0	
Response	
Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 3	
Answer	Yes
Document Name	
Comment	
PNM Resources supports EEI’s comments on this question.	
Likes 0	
Dislikes 0	
Response	
Warren Cross - ACES Power Marketing - 1,3,4,5 - MRO,WECC,Texas RE,SERC	
Answer	Yes
Document Name	
Comment	
No comments.	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1	
Answer	Yes
Document Name	
Comment	

We feel that the example presented in the Technical Guidance reflects the Exemption accurately, however, the SDT is compounding the Control Center issue by having another explanation of a Control Center/control center to those already present in CIP-002, CIP-014, and the NERC Glossary, and now CIP-012. We recommend a single document that explains the Control Center / control center topic.

Likes 0	
Dislikes 0	

Response

Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran

Answer	Yes
Document Name	

Comment

Oncor supports EEI's comment.

Likes 0	
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	Yes
Document Name	

Comment

Southern Company supports the need to exempt certain Control Centers. Barring the ability to address the Control Center definition fully, Southern recognizes that the proposed Standard addresses the need for an exemption in an appropriate way.

Likes 0	
Dislikes 0	

Response

Andrea Koch - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	Yes
Document Name	CIP 12 Figures.pdf

Comment

EEI supports the need for an exemption and explanation for digital control systems installed at generating stations and Transmission stations and substations that may also be classified as Control Centers. However, we have concerns that some parts of the Technical Rationale may align too closely with NERC's description of Implementation Guidance. (see Technical Rationale Transition Plan)

In the redline edits provided by the SDT, Figures 2 and 3 provide examples of communications between two generating stations, while technically conforming to the definition of a Control Center, are outside the intended scope of CIP-012-1 standard. While the language and figures provide needed clarity, we suggest the SDT consider using diagrams that more closely conforms to the figures provided within our comments. We have provided these suggested changes because we are concerned that the issues of aggregated communications along with situations where Facilities contained within a single confined area are not clearly addressed in the Technical Rationale. We believe the diagrams provided more clearly define the limitations of the exemption.

As stated above, we are concerned that the examples and approaches provided in the Technical Rationale may be better contained in the Implementation Guidance given the above referenced NERC document suggests that Implementation Guidance is where examples and approaches are to be used to illustrate how to comply with a Reliability Standard.

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion

Answer	Yes
Document Name	

Comment

We feel that the example presented in the Technical Guidance reflects the Exemption accurately, however, the SDT is compounding the Control Center issue by having another explanation of a Control Center/control center to those already present in CIP-002, CIP-014, and the NERC Glossary, and now CIP-012. We recommend a single document that explains the Control Center / control center topic.

Likes 0	
Dislikes 0	

Response

Eli Rivera - Central Electric Cooperative, Inc. (Redmond, Oregon) - NA - Not Applicable - Texas RE

Answer	Yes
Document Name	

Comment

CenterPoint Energy Houston Electric, LLC ("CenterPoint Energy") agrees with Edison Electric Institute's (EEI) comments.

Likes 0	

Dislikes 0	
Response	
Chris Scanlon - Exelon - 1	
Answer	Yes
Document Name	
Comment	

Exelon supports the need for an exemption and explanation for digital control systems installed at generating stations and Transmission stations and substations that may also be classified as Control Centers. However, we have concerns that some parts of the Technical Rationale may align too closely with NERC's description of Implementation Guidance. (see Technical Rationale Transition Plan)

In the redline edits provided by the SDT, Figures 2 and 3 provide examples of communications between two generating stations, while technically conforming to the definition of a Control Center, are outside the intended scope of CIP-012-1 standard. While the language and figures provide needed clarity, we suggest the SDT consider using diagrams that more closely conform to the figures provided within our comments. We have provided these suggested changes because we are concerned that the issues of aggregated communications along with situations where Facilities contained within a single confined area are not clearly addressed in the Technical Rationale. We believe the diagrams provided more clearly define the limitations of the exemption.

Exelon is also concerned that the examples and approaches provided in the Technical Rationale may be better contained in the Implementation Guidance given the above referenced NERC document suggests that Implementation Guidance is where examples and approaches are to be used to illustrate how to comply with a Reliability Standard.

Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	

NV Energy understands that a unknown expedited timeline and the original SAR are obstacles for the SDT at this time, and that this Standard will be approved in the near term, but we believe that further development of the Control Center definition should be resolved before more standards regarding Control Centers are introduced.

Likes 0	
Dislikes 0	
Response	

Darnez Gresham - Darnez Gresham On Behalf of: Annette Johnston, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Darnez Gresham	
Answer	Yes
Document Name	
Comment	
While MEC understands that time and the SAR are obstacles for the SDT at this time, however, issues with the existing Control Center definition should be resolved before more standards regarding Control Centers are introduced.	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
PAC understands that time and the SAR are obstacles for the SDT at this time, further development of the Control Center definition should be resolved before more standards regarding Control Centers are introduced.	
Likes 0	
Dislikes 0	
Response	
Russell Martin II - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
SRP agrees with the Technical Rationale and Justification for CIP-012 provided by the SDT. However, SRP continues to maintain that an additional 12 months be considered for the plan implementation aspect of Requirement R1. PDF page 6, paragraph 3 of section title *Identification of Where Security Protection is Applied by the Responsible Entity* states "The SDT understands that in data exchanges between Control Centers, a single entity may not be responsible for both ends of the communication link." With the intent of the standard being to secure communications between Control Centers (including communication between two separate entities Control Centers), this will call for inter-entity cooperation to ensure both sides of link are secure. This is where the additional 12 months would be necessary, for coordination of efforts from both entities.	
Likes 0	

Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5	
Answer	Yes
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	
Dennis Sismaet - Northern California Power Agency - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Marty Hostler - Northern California Power Agency - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 5,6	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Wagner - Santee Cooper - 1, Group Name Santee Cooper	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Douglas Johnson - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Jeff Johnson - Jeff Johnson On Behalf of: Martine Blair, Sempra - San Diego Gas and Electric, 3, 5, 1; - Jeff Johnson	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb On Behalf of: Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; James McBee, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; Jessica Tucker, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; Jim Flucke, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; Megan Wagner, Westar Energy, 6, 3, 1, 5; - Douglas Webb	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Shaw - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

David Ramkalawan - Ontario Power Generation Inc. - 5	
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	
Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 3, Group Name FirstEnergy Corporation	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aubrey Short - FirstEnergy - FirstEnergy Corporation - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Maier - Intermountain REA - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steve Rose - City Water, Light and Power of Springfield, IL - 1,3,5	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE does not have comments on this question.	
Likes 0	
Dislikes 0	
Response	

5. The SDT modified the draft Implementation Guidance for CIP-012 to provide examples of how a Responsible Entity could comply with the requirements. The draft Implementation Guidance does not prescribe the only approaches to compliance. Rather, it describes what the SDT believes would be effective ways to comply with the standard. See NERC's Compliance Guidance policy for information on Implementation Guidance. Do you agree with the draft Implementation Guidance? If you do not agree, or if you agree but have comments or suggestions for the draft Implementation Guidance, please provide your recommendation and explanation.

Thomas Foltz - AEP - 5	
Answer	No
Document Name	

Comment

AEP requests the SDT consider including some statements in the Implementation Guidance to address the possibility that data requests made related to TOP-003 and/or IRO-010 include other data that is not Real-time Assessment data or Real-time monitoring data, and how the Responsible Entity could exclude this other data from the security requirements.

Likes 0	
Dislikes 0	

Response

Russell Martin II - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	

Comment

Overall, SRP does not agree with twenty-four (24) calendar months for the implementation of Requirements R1, as R1 and R2 from the second draft have been merged. Although SRP recognizes the SDT is not specifying the controls to be used to protect confidentiality and integrity, the only examples provided in the implementation guidance includes encryption. If there are other methods available to achieve the security objective, SRP asks the SDT to provide them. However, the only method available to achieve the proposed required objective, on the ICCP network, is to implement encryption. As FERC order 822 states on page 37, "if several registered entities have joint responsibility for a cryptographic key management system used between their respective Control Centers, they should have the prerogative to come to a consensus on which organization administers that particular key management system." Furthermore, the FERC order states on page 38, "While responsible entities are required to exchange real-time and operational planning data necessary to operate the bulk electric system using mutually agreeable security protocols, there is no technical specification for how this transfer of information should incorporate mandatory security controls." These are activities and specifications that must be created and agreed upon by all registered entities involved in the data transfer. As such the timeline is reliant on registered entities working together on a common solution and would not be achievable within 24 calendar months.

Additionally, if encryption fails, SRP would lose Real-time Assessment and Real-time monitoring and control data. There are many opportunities for encryption to fail that must be addressed. The implementation of encryption requires a pilot to truly understand and address the mechanisms of failure, the impacts encryption would cause on the exchange of the data, and the computing resources required. A pilot also requires a great amount of coordination to execute, not only within the industry, but may also include carriers, vendors, and possibly third-party encryption key program managers.

Because of the aforementioned reasons and concerns, SRP is recommending a phased implementation for CIP-012-1. A 24 month implementation is appropriate, but only for Requirement R1. The 24 months for R1 would provide time to coordinate and create an industry-wide solution. SRP is

proposing the SDT include an additional 12 months for the plan implementation aspect of Requirement R1. The additional 12 months would be used for a pilot and course correction if needed, in addition to understanding, formulating, and executing maintenance strategies.

Likes 0	
Dislikes 0	

Response

Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	No
Document Name	

Comment

Based upon NSRF comments to delete Requirement 1, Part 1.3 as identified under #2 of this comment form, the section within the Implementation Guidance titled “Identification of Responsibilities when the Control Centers are Owned or Operated by Different Responsible Entities” would need to be revised or eliminated. In addition, the Reference Model section of the Implementation Guide would also need be revised in those areas that reflect Responsible Entity accountability for other Responsible Entities.

The drafting team in earlier response to comments has stated that the Implementation Guidance would be submitted as a Standard Application Guide to NERC. This is imperative for Responsible Entities and Regional Entities to understand the intent and consistent application of this non-prescriptive Standard.

The NSRF questions when any type of Guidance is needed when the Standard is clearly written. As stated in FERC Order 693 section 253, FERC states “…The most critical element of a Reliability Standard is the Requirements. As NERC explains, “the Requirements within a standard define what an entity must do to be compliant . . . [and] binds an entity to certain obligations of performance under section 215 of the FPA.” If properly drafted, a Reliability Standard may be enforced in the absence of specified Measures or Levels of Non-Compliance”.

Likes 0	
Dislikes 0	

Response

David Jendras - Ameren - Ameren Services - 1,3,6

Answer	No
Document Name	

Comment

As with technical rationale any implementation guidance that can be condensed into clear, concise language should be moved into the CIP-012-1 as a defined requirement. Responsible Entities are audited to the Requirements in the Standard. In our opinion, leaving this much information as implementation guidance invites subjective audit interpretation and therefore unnecessarily increases compliance risk for the entity. The inclusion of acceptable means/methods within the verbiage of a Requirement does not necessarily make it prescriptive because the wording can state "or any other means that addresses the XXX risk". In addition, this type of guidance provides explicit compliance help which on its face increases overall BES reliability because entities may rely on the guidance to be compliant and not err by misinterpreting what can be done.

Likes 0	
Dislikes 0	
Response	
Aaron Smith - Omaha Public Power District - 1,3,5,6	
Answer	No
Document Name	
Comment	
: Based upon NSRF comments to delete Requirement 1, Part 1.3 as identified under #2 of this comment form the section within the Implementation Guidance titled “Identification of Responsibilities when the Control Centers are Owned or Operated by Different Responsible Entities” would need to be revised or eliminated. In addition, the Reference Model section of the Implementation Guide would also need be revised in those areas that reflect Responsible Entity accountability for other Responsible Entities. The drafting team in earlier response to comments has stated that the Implementation Guidance would be submitted as a Standard Application Guide to NERC. This is imperative for Resonsible Entities and Regional Entities to understand intent and consistent application of this non-prescriptive Standard. The NSRF questions when any type of Guidance is needed when the Standard is clearly written. As stated in FERC Order 693 section 253, FERC states “…The most critical element of a Reliability Standard is the Requirements. As NERC explains, “the Requirements within a standard define what an entity must do to be compliant . . . [and] binds an entity to certain obligations of performance under section 215 of the FPA.” If properly drafted, a Reliability Standard may be enforced in the absence of specified Measures or Levels of Non-Compliance	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,4,5 - RF	
Answer	No
Document Name	
Comment	
In the Implementation Guidance document, please specify what type of date under TOP-003 and IRO-010 should be excluded from the CIP-012 requirements.	
Likes 0	
Dislikes 0	
Response	

Brandon McCormick - Brandon McCormick On Behalf of: Ginny Beigel, City of Vero Beach, 3; Lynne Mila, City of Clewiston, 4; Mike Blough, Kissimmee Utility Authority, 5, 3; Tom Reedy, Florida Municipal Power Pool, 6; - Brandon McCormick, Group Name FMPA	
Answer	No
Document Name	
Comment	
The example “Identification of Responsibilities when the Control Centers are Owned or Operated by Different Responsible Entities, the language indicates the communication link endpoint is within a PSP. If the Control Center is rated as a Low Impact per the CIP-002-5.1a Attachment 1 Criteria 3.1, the term PSP does not apply and is not required by the Standard.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb On Behalf of: Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; James McBee, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; Jessica Tucker, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; Jim Flucke, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; Megan Wagner, Westar Energy, 6, 3, 1, 5; - Douglas Webb	
Answer	No
Document Name	
Comment	
Kansas City Power and Light Company incorporates the Edison Electric Institute's response to Question No. 5.	
Likes 0	
Dislikes 0	
Response	
Richard Montgomery - Florida Municipal Power Agency - 3,4,5,6	
Answer	No
Document Name	
Comment	
The example “Identification of Responsibilities when the Control Centers are Owned or Operated by Different Responsible Entities, the language indicates the communication link endpoint is within a PSP. If the Control Center is rated as a Low Impact per the CIP-002-5.1a Attachment 1 Criteria 3.1, the term PSP does not apply and is not required by the Standard	
Likes 0	
Dislikes 0	

Response	
Carol Chinn - Florida Municipal Power Agency - 3,4,5,6	
Answer	No
Document Name	
Comment	
The example “Identification of Responsibilities when the Control Centers are Owned or Operated by Different Responsible Entities, the language indicates the communication link endpoint is within a PSP. If the Control Center is rated as a Low Impact per the CIP-002-5.1a Attachment 1 Criteria 3.1, the term PSP does not apply and is not required by the Standard	
Likes 0	
Dislikes 0	
Response	
Joe McKinney - Florida Municipal Power Agency - 3,4,5,6	
Answer	No
Document Name	
Comment	
The example “Identification of Responsibilities when the Control Centers are Owned or Operated by Different Responsible Entities, the language indicates the communication link endpoint is within a PSP. If the Control Center is rated as a Low Impact per the CIP-002-5.1a Attachment 1 Criteria 3.1, the term PSP does not apply and is not required by the Standard.	
Likes 0	
Dislikes 0	
Response	
Chris Gowder - Florida Municipal Power Agency - 3,4,5,6	
Answer	No
Document Name	
Comment	
The example “Identification of Responsibilities when the Control Centers are Owned or Operated by Different Responsible Entities, the language indicates the communication link endpoint is within a PSP. If the Control Center is rated as a Low Impact per the CIP-002-5.1a Attachment 1 Criteria 3.1, the term PSP does not apply and is not required by the Standard	
Likes 0	

Dislikes 0	

Response

Chris Scanlon - Exelon - 1

Answer	No
Document Name	

Comment

Generally, Exelon supports the Implementation Guidance, but ask the SDT to consider the following suggested changes:

1. Address how an entity might effectively identify Control Centers (as defined by the NERC Glossary) that would be exempted from complying with CIP-012-1 as a result of the newly developed Exemption 4.2.3 language.

2. There are many different approaches to mitigating the risk of unauthorized disclosure or modification of data in transit. Additional guidance that explores various approaches and evaluates their effectiveness in mitigating risk may be helpful before entities make implementation investments for CIP-012-1.

3. Exelon suggests the SDT consider removing or modifying the email example (last bullet on page 8) since email and the associated password exchange recommended (e.g., by phone) i “inconsistent with the requirements of Real-time data exchange” as indicated in the draft Implementation Guidance.

While Exwlon recognizes that approval of Implementation Guidance goes beyond the responsibility of the SDT, we suggest the final version of Implementation Guidance be approved by the ERO and posted with the Standard before any final ballot.

Likes 0	
Dislikes 0	

Response

Stephanie Burns - Stephanie Burns On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Stephanie Burns

Answer	No
Document Name	

Comment

Comments above in question 4 apply here as well.

Likes 0	
Dislikes 0	

Response

Eli Rivera - Central Electric Cooperative, Inc. (Redmond, Oregon) - NA - Not Applicable - Texas RE	
Answer	No
Document Name	
Comment	
CenterPoint Energy Houston Electric, LLC (“CenterPoint Energy”) agrees with Edison Electric Institute’s (EEI) comments.	
Likes 0	
Dislikes 0	
Response	

Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	No
Document Name	
Comment	
Please refer to MRO NERC Standards Review Forum (NSRF) comments.	
Likes 0	
Dislikes 0	
Response	

James Anderson - CMS Energy - Consumers Energy Company - 1	
Answer	No
Document Name	
Comment	
In the Implementation Guidance document, please specify what type of date under TOP-003 and IRO-010 should be excluded from the CIP-012 requirements.	
Likes 0	
Dislikes 0	
Response	

Andrea Koch - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No

Document Name	

Comment

Generally, EEI supports the Implementation Guidance, but ask the SDT to consider the following suggested changes:

1. Address how an entity might effectively identify Control Centers (as defined by the NERC Glossary) that would be exempted from complying with CIP-012-1 as a result of the newly developed Exemption 4.2.3 language.

2. There are many different approaches to mitigating the risk of unauthorized disclosure or modification of data in transit. Additional guidance that explores various approaches and evaluates their effectiveness in mitigating risk may be helpful before entities make implementation investments for CIP-012-1.

3. EEI suggests the SDT consider removing or modifying the email example (last bullet on page 8) since email and the associated password exchange recommended (e.g., by phone) i "inconsistent with the requirements of Real-time data exchange" as indicated in the draft Implementation Guidance.

While EEI recognizes that approval of Implementation Guidance goes beyond the responsibility of the SDT, we suggest the final version of Implementation Guidance be approved by the ERO and posted with the Standard before any final ballot.

Likes 0	
Dislikes 0	

Response

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

On pages 5 and 6 of the Implementation Guidance document, BPA believes additional clarity is needed to identify each entity's responsibility, as follows: "Where the operational obligations of an entire communication link, including both endpoints, belong to the Control Center of another Responsible Entity **A**, the Responsible Entity without operational obligations **(B)** for the communication link **Responsible Entity B** may demonstrate compliance by ensuring the communications link endpoint is within **B's** Control Center, which could be limited to including the communication link endpoint within **B's** PSP."

Likes 0	
Dislikes 0	

Response

Chris Wagner - Santee Cooper - 1, Group Name Santee Cooper

Answer	No
Document Name	

Comment
The guidance provides encryption as a method. The industry has not been able to test security controls such as encryption, to ensure that reliability is not impacted. Concerned that encryption of data will create an adverse impact to reliability. It is unclear the amount of latency that may be added or amount of computing resources required to encrypt and decrypt this data every 6 seconds. Additionally, the burden should not be placed on a Registered Entity to prove that a neighbor's control room has the appropriate protections in place. We should only have the burden for our own control room.

Likes 0	
Dislikes 0	

Response

David Greyerbiehl - CMS Energy - Consumers Energy Company - 5	
Answer	No
Document Name	

Comment
In the Implementation Guidance document, please specify what type of date under TOP-003 and IRO-010 should be excluded from the CIP-012 requirements.

Likes 0	
Dislikes 0	

Response

Marty Hostler - Northern California Power Agency - 5	
Answer	No
Document Name	

Comment
IRO-010-2 R3.3 and TOP-003-3 R5.3 already provide reliability assurance requirements for RCs, BAs, GOs, GOPs, TOPs, TOs, and DPs; and they are not presriptive. Consequently, CIP-012 is and its' draft implementation quidance are not needed. Additionally, NERC has a Standards Efficiency Initiative underway to get rid of standards and requirements such as CIP-012-1 and its' Requirement 1.

Likes 0	
Dislikes 0	

Response

Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	
Comment	
IRO-010-2 R3.3 and TOP-003-3 R5.3 already provide reliability assurance requirements for RCs, BAs, GOs, GOPs, TOPs, TOs, and DPs; and they are not prescriptive. Consequently, CIP-012 is and its' draft implementation guidance are not needed. Additionally, NERC has a Standards Efficiency Initiative underway to get rid of standards and requirements such as CIP-012-1 and its' requirement 1.	
Likes 0	
Dislikes 0	
Response	

Tho Tran - Tho Tran On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Tho Tran	
Answer	No
Document Name	
Comment	
Oncor supports EEI's comment.	
Likes 0	
Dislikes 0	
Response	

David Francis - Midcontinent ISO, Inc. - 2 - MRO,SERC,RF	
Answer	No
Document Name	
Comment	
For the same reasons stated in response for question 4 with third party personnel entering a PSP	
Likes 0	
Dislikes 0	
Response	

Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 3

Answer	No
Document Name	
Comment	
PNM Resources supports EEI's comments on this question.	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5	
Answer	Yes
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
PacifiCorp agrees with modifications made to the implementation guidance, specifically the newly introduced paragraph, "Where the operational obligations of an entire communication link, including both endpoints, belong to the Control Center of another Responsible Entity, the Responsible Entity without operational obligations for the communication link may demonstrate compliance by ensuring the communications link endpoint is within its Control Center, which could be limited to including the communication link endpoint within a PSP." PacifiCorp would like the following edit added "or where other physical protections are applied." PacifiCorp feels that this will allow entities flexibility where the devices that perform this are located within its location. PacifiCorp also likes the VPN examples provided. If the newly introduced paragraph or the VPN examples are removed or if the implementation guidance is not ERO-endorsed prior to the final ballot, PacifiCorp may alter its final vote.	
Likes 0	
Dislikes 0	
Response	

Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	

Darnez Gresham - Darnez Gresham On Behalf of: Annette Johnston, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Darnez Gresham	
Answer	Yes
Document Name	
Comment	
MEC agrees with modifications made to the Implementation Guidance, specifically the newly introduced sentence, “Where the operational obligations of an entire communication link, including both endpoints, belong to the Control Center of another Responsible Entity, the Responsible Entity without operational obligations for the communication link may demonstrate compliance by ensuring the communications link endpoint is within its Control Center, which could be limited to including the communication link endpoint within a PSP.” MEC would like to see “or where other physical protections are applied.” This will provide more flexibility for entities. MEC also likes the VPN example provided. Inclusion of the newly introduced sentence, the VPN example and ERO-endorsement of the implementation guidance are needed in the final version for MEC to vote yes on the final ballot.	
Likes 0	
Dislikes 0	
Response	

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
NV Energy agrees with the requirement based on the newly introduced paragraph in the Implementation Guidance, “Where the operational obligations of an entire communication link, including both endpoints, belong to the Control Center of another Responsible Entity, the Responsible Entity without operational obligations for the communication link may demonstrate compliance by ensuring the communications link endpoint is within its Control Center, which could be limited to including the communication link endpoint within a PSP.” NV Energy would like the following edit added “or where other physical protections are applied.” NV Energy believes that this will allow entities flexibility where their devices that perform this function are located within its location. NV Energy believes the VPN examples provided are necessary and should	

remain within the Guidance document. If the newly introduced paragraph or the VPN example are removed or if the implementation guidance is not ERO-endorsed prior to the final ballot, NV Energy may alter its final vote.	
Likes 0	
Dislikes 0	
Response	
Douglas Johnson - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
American Transmission Company LLC (ATC) agrees that the controls prescribed by CIP-006 satisfy CIP-012 Requirement R1 Parts 1.1 and 1.2, and appreciates being able to leverage Standards that are already implemented and enforceable as opposed to creating a new requirement. ATC cautions that this approach could re-create 'spaghetti' requirements placing Registered Entities in potential double jeopardy if conditions of non-compliance occur. ATC requests consideration of inclusion of statements in a CIP-012 CMEP Practice Guide to instruct Regional Compliance Enforcement Agencies to audit in a manner that does not place the Registered Entities at odds with both CIP-006-6 and CIP-012 for individual instances of potential non-compliance.	
Likes 0	
Dislikes 0	
Response	
Warren Cross - ACES Power Marketing - 1,3,4,5 - MRO,WECC,Texas RE,SERC	
Answer	Yes
Document Name	
Comment	
No comments.	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - MRO, Group Name SPP Standards Review Group	
Answer	Yes
Document Name	

Comment
The SPP Standards Review Group would ask that the drafting team provide us some feedback on the next steps in their process on how they plan to get the Implementation Guidance Document formalized and coordinated with the CIP-012-1 Standard. From our prospective, this document was well put together and we would hate to see this document to be left out of the approval process for the CIP project.

Likes 0	
Dislikes 0	

Response

Steve Rose - City Water, Light and Power of Springfield, IL - 1,3,5	
Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

David Maier - Intermountain REA - 3	
Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Aubrey Short - FirstEnergy - FirstEnergy Corporation - 4	
Answer	Yes
Document Name	

Comment

Likes 0	

Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 3, Group Name FirstEnergy Corporation	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
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	
David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Shaw - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeff Johnson - Jeff Johnson On Behalf of: Martine Blair, Sempra - San Diego Gas and Electric, 3, 5, 1; - Jeff Johnson	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1	
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	
Document Name	
Comment	
No comment at this time.	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE prefers commenting on Implementation Guidance once the standard language is in its final form.	
Likes 0	
Dislikes 0	
Response	

6. The SDT believes proposed CIP-012-1 provides entities with flexibility to meet the reliability objectives in a cost effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost effective approaches, please provide your recommendation and, if appropriate, technical justification.

Dennis Sismaet - Northern California Power Agency - 6

Answer	No
Document Name	

Comment

IRO-010-2 R3.3 and TOP-003-3 R5.3 already provide reliability assurance requirements for RCs, BAs, GOs, GOPs, TOPs, TOs, and DPs; they provide flexibility to meet reliability objectives in a cost effective manner. Proposed CIP-012 does not, and is not needed. Additionally, NERC has a Standards Efficiency Initiative underway to get rid of standards and requirements such as CIP-012-1 and its' Requirement 1.

Likes 0	
Dislikes 0	

Response

Marty Hostler - Northern California Power Agency - 5

Answer	No
Document Name	

Comment

IRO-010-2 R3.3 and TOP-003-3 R5.3 already provide reliability assurance requirements for RCs, BAs, GOs, GOPs, TOPs, TOs, and DPs; they provide flexibility to meet reliability objectives in a cost effective manner. Proposed CIP-012 does not and is not needed. Additionally, NERC has a Standards Efficiency Initiative underway to get rid of standards and requirements such as CIP-012-1 and its' Requirement 1.

Likes 0	
Dislikes 0	

Response

David Greyerbiehl - CMS Energy - Consumers Energy Company - 5

Answer	No
Document Name	

Comment

More flexibility and less guidance could lead to inconsistency on requirement implementation among different entities.

Likes 0	
Dislikes 0	

Response

Chris Wagner - Santee Cooper - 1, Group Name Santee Cooper

Answer	No
Document Name	

Comment

Significant capital may need to be budgeted in order to implement architecture improvements to address the required computing resources for encryption and decryption of data. Encryption adds a burden for on-going maintenance and management. There is concern of the impacts on real-time operations for encryption and decryption of data.

Likes 0	
Dislikes 0	

Response

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

BPA believes that if the data must be protected throughout the transmission, it would seem that could only be accomplished with encryption. For cases where the existing equipment is not capable of encryption, replacement will be costly and implementation lengthy. While the proposed standard and implementation guidance do not require encryption, no other solution seems viable.

Due to BPA's large amount of applicable data, access to funds and budget cycle, and resources to perform work required, the solution will be costly.

BPA also agrees with SRP's comments as follows:

"SRP does not agree the current standard and implementation plan can be executed in a cost effective manner. Encryption has been the only presented solution provided by auditors and SDT guidance to protect both confidentiality and integrity for the data within this scope. If the implementation timeframe remains at 24 months, more resources and capital will be required versus a phased implementation. A phased implementation provides the ability to not only ensure the most effective plan, but also provides the ability to plan more accurately within budget cycles. More importantly, if encryption fails, SRP would lose Real-time Assessment and Real-time monitoring and control data. SRP is concerned a 24 month implementation timeline would impact reliability as there are many opportunities for encryption to fail that must be addressed. This has a direct correlation on cost when addressing those opportunities during this timeframe.

Additionally, SRP would like to see reference models of methods that do not require encryption as a method to protect communications between Control Centers.”	
Likes 0	
Dislikes 0	
Response	
James Anderson - CMS Energy - Consumers Energy Company - 1	
Answer	No
Document Name	
Comment	
More flexibility and less guidance could lead to inconsistency on requirement implementation among different entities.	
Likes 0	
Dislikes 0	
Response	
Stephanie Burns - Stephanie Burns On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Stephanie Burns	
Answer	No
Document Name	
Comment	
ITC does not agree with this approach being cost effective. This is especially true for larger balancing authorities that own and pay for many routers and circuits to receive ICCP data they require for real time operation. Many routers deployed today may not have encryption capabilities and many circuits may not have adequate bandwidth to support additional encryption overhead. In addition the methods to connect to the control center such as the lease lines, or communication circuits, may need to change to accommodate the new protection requirements.	
Likes 0	
Dislikes 0	
Response	
Chris Gowder - Florida Municipal Power Agency - 3,4,5,6	
Answer	No
Document Name	
Comment	

Undetermined	
Likes 0	
Dislikes 0	
Response	
Joe McKinney - Florida Municipal Power Agency - 3,4,5,6	
Answer	No
Document Name	
Comment	
Undetermined	
Likes 0	
Dislikes 0	
Response	
Carol Chinn - Florida Municipal Power Agency - 3,4,5,6	
Answer	No
Document Name	
Comment	
Undetermined	
Likes 0	
Dislikes 0	
Response	
Richard Montgomery - Florida Municipal Power Agency - 3,4,5,6	
Answer	No
Document Name	
Comment	
Undetermined	

Likes 0	
Dislikes 0	
Response	
Brandon McCormick - Brandon McCormick On Behalf of: Ginny Beigel, City of Vero Beach, 3; Lynne Mila, City of Clewiston, 4; Mike Blough, Kissimmee Utility Authority, 5, 3; Tom Reedy, Florida Municipal Power Pool, 6; - Brandon McCormick, Group Name FMPA	
Answer	No
Document Name	
Comment	
Undetermined	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,4,5 - RF	
Answer	No
Document Name	
Comment	
More flexibility and less guidance could lead to inconsistency on requirement implementation among different entities.	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	No
Document Name	
Comment	
Reclamation recommends the term “plan” be replaced with the term “process” throughout the CIP-012-1 standard, Technical Rationale, Implementation Guidance, and associated documents. A plan is an unwarranted layer of compliance that does not improve the reliability of the BES. The processes an entity implements have defined controls that reduce the entity’s risks to the BES and thereby improve BES reliability.	

Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 1,3,6	
Answer	No
Document Name	
Comment	
As currently worded in draft 4 we believe that there is too much potential risk to support a "yes" response to this question.	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	No
Document Name	
Comment	
The options for flexibility aren’t clearly presented in the draft standard and the language provided.	
Likes 0	
Dislikes 0	
Response	
Russell Martin II - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
SRP does not agree the current standard and implementation plan can be executed in a cost effective manner. Encryption has been the only presented solution provided by auditors and SDT guidance to protect both confidentiality and integrity for the data within this scope. If the implementation timeframe remains at 24 months, more resources and capital will be required versus a phased implementation. A phased implementation provides the ability to not only ensure the most effective plan, but also provides the ability to plan more accurately within budget cycles. More importantly, if encryption fails, SRP would lose Real-time Assessment and Real-time monitoring and control data. SRP is concerned a 24 month implementation	

timeline would impact reliability as there are many opportunities for encryption to fail that must be addressed. This has a direct correlation on cost when addressing those opportunities during this timeframe.

Additionally, SRP would like to see reference models of methods that do not require encryption as a method to protect communications between Control Centers.

Likes 0	
Dislikes 0	

Response

Warren Cross - ACES Power Marketing - 1,3,4,5 - MRO,WECC,Texas RE,SERC

Answer	Yes
Document Name	

Comment

ACES does agree with the cost effective approach, if the wording is revised from Control Center to Facility. A Control Center has much more compliance obligations than a Facility.

Likes 0	
Dislikes 0	

Response

Teresa Cantwell - Lower Colorado River Authority - 1,5

Answer	Yes
Document Name	

Comment

None

Likes 0	
Dislikes 0	

Response

David Francis - Midcontinent ISO, Inc. - 2 - MRO,SERC,RF

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Douglas Johnson - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeff Johnson - Jeff Johnson On Behalf of: Martine Blair, Sempra - San Diego Gas and Electric, 3, 5, 1; - Jeff Johnson	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Darnez Gresham On Behalf of: Annette Johnston, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Darnez Gresham	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb On Behalf of: Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; James McBee, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; Jessica Tucker, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; Jim Flucke, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; Megan Wagner, Westar Energy, 6, 3, 1, 5; - Douglas Webb	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Shaw - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
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	
Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 3, Group Name FirstEnergy Corporation	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aubrey Short - FirstEnergy - FirstEnergy Corporation - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

David Maier - Intermountain REA - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thomas Foltz - AEP - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steve Rose - City Water, Light and Power of Springfield, IL - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - MRO, Group Name SPP Standards Review Group	
Answer	
Document Name	
Comment	

N/A	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE does not have comments on this question.	
Likes 0	
Dislikes 0	
Response	
Andrea Koch - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	
Document Name	
Comment	
No comment	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	
Document Name	
Comment	
This has not been determined due to the need for revisions to the proposed standard.	

Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	
Document Name	
Comment	
No comment at this time.	
Likes 0	
Dislikes 0	
Response	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	
Document Name	
Comment	
Undetermined at this time.	
Likes 0	
Dislikes 0	
Response	

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Reminder

Project 2016-02 Modifications to CIP Standards

Additional Ballot and Non-binding Polls Open through July 2, 2018

Now Available

The additional ballot and non-binding Poll for **CIP-012-1 – Cyber Security - Communications between Control Centers** is open through **8 p.m. Eastern, Monday, July 2, 2018.**

The standard drafting team's considerations of the responses received from the last comment period reflected in this draft of the standard.

Balloting

Members of the ballot pools associated with this project can log in to the Standards Balloting and Commenting System (SBS) and submit their votes. If you experience difficulty navigating the SBS, contact Wendy Muller.

- *If you are having difficulty accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out, contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern).*
- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*
- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Note: If a member cast a vote in the previous ballot, that vote will not carry over to the additional ballot. It is the responsibility of the registered voter in the ballot pool to cast a vote again in the additional ballot. To ensure a quorum is reached, if you do not want to vote affirmative or negative, cast an abstention.

Next Steps

The ballot results will be announced and posted on the project page. The drafting team will review all responses received during the comment period and determine the next steps of the project.

For information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact Standards Developer, Jordan Mallory (via email) or at (404) 446-2589.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2016-02 Modifications to CIP Standards

Formal Comment Period Open through July 2, 2018

Now Available

A 45-day formal comment period for **CIP-012-1 – Cyber Security - Communications between Control Centers** is open through **8 p.m. Eastern, Monday, July 2, 2018.**

The Technical Rationale and Implementation Guidance Documents for CIP-012-1 will be posted within 15 days of the comment period opening.

Additionally, the CIP standard drafting team (SDT) proposed a revised Control Center definition during the March 16 – April 30, 2018 comment and ballot period. Based on feedback received from industry, the SDT decided to draft exemption language within the applicability section of CIP-012 instead of revising the Control Center definition. Please see the Control Center definition consideration of comments report for additional SDT responses on the new path taken by the SDT.

Commenting

Use the Standards Balloting and Commenting System (SBS) to submit comments. If you experience difficulties navigating the SBS, contact Wendy Muller. An unofficial Word version of the comment form is posted on the project page.

- *If you are having difficulty accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out, contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern).*
- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*
- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Next Steps

An additional ballot for the Standard and a non-binding poll of the associated Violation Risk Factors and Violation Severity Levels will be conducted **June 22 – July 2, 2018.**

For information on the Standards Development Process, refer to the Standard Processes Manual**.**

For more information or assistance, contact Standards Developer, Jordan Mallory at (404) 446-2589.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/136)
Ballot Name: 2016-02 Modifications to CIP Standards CIP-012-1 AB 4 ST
Voting Start Date: 6/22/2018 12:01:00 AM
Voting End Date: 7/3/2018 8:00:00 PM
Ballot Type: ST
Ballot Activity: AB
Ballot Series: 4
Total # Votes: 233
Total Ballot Pool: 309
Quorum: 75.4
Weighted Segment Value: 68.45

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	80	1	41	0.661	21	0.339	0	3	15
Segment: 2	7	0.5	4	0.4	1	0.1	0	1	1
Segment: 3	73	1	36	0.692	16	0.308	0	4	17
Segment: 4	17	1	8	0.8	2	0.2	0	1	6
Segment: 5	73	1	24	0.533	21	0.467	0	2	26
Segment: 6	46	1	18	0.563	14	0.438	0	5	9
Segment: 7	2	0	0	0	0	0	0	1	1
Segment: 8	3	0.2	2	0.2	0	0	0	0	1
Segment: 9	1	0.1	1	0.1	0	0	0	0	0
Segment: 10	7	0.7	5	0.5	2	0.2	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Totals:	309	6.5	139	4.449	77	2.051	0	17	76

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Affirmative	N/A
1	Allete - Minnesota Power, Inc.	Jamie Monette		Abstain	N/A
1	American Transmission Company, LLC	Douglas Johnson		Affirmative	N/A
1	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	John Shaver		None	N/A
1	Associated Electric Cooperative, Inc.	Ryan Ziegler		Affirmative	N/A
1	Austin Energy	Thomas Standifur		None	N/A
1	Balancing Authority of Northern California	Kevin Smith	Joe Tarantino	Affirmative	N/A
1	Basin Electric Power Cooperative	David Rudolph		None	N/A
1	BC Hydro and Power Authority	Patricia Robertson		Affirmative	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Bonneville Power Administration	Kammy Rogers-Holliday		Negative	Comments Submitted
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		Negative	Third-Party Comments
1	Cedar Falls Utilities	Adam Peterson		None	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Hudson Gas & Electric Corp.	Frank Pace		Affirmative	N/A
1	City Utilities of Springfield, Missouri	Michael Buyce		None	N/A
1	CMS Energy - Consumers Energy Company	James Anderson		Negative	Comments Submitted
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Larry Nash		Affirmative	N/A
1	Duke Energy	Laura Lee		Negative	Comments Submitted
1	Edison International - Southern California Edison Company	Steven Mavis		Affirmative	N/A
1	Entergy - Entergy Services, Inc.	Oliver Burke		Affirmative	N/A
1	Eversource Energy	Quintin Lee		Affirmative	N/A
1	Exelon	Chris Scanlon		Negative	Comments Submitted
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A
1	Great Plains Energy - Kansas City Power and Light Co.	James McBee	Douglas Webb	Negative	Third-Party Comments
1	Great River Energy	Gordon Pietsch		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Affirmative	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Affirmative	N/A
1	IDACORP - Idaho Power Company	Laura Nelson		Negative	Comments Submitted
1	Imperial Irrigation District	Jesus Sammy Alcaraz		None	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Stephanie Burns	Negative	Comments Submitted
1	Lincoln Electric System	Danny Pudenz		Negative	Third-Party Comments
1	Long Island Power Authority	Robert Ganley		Affirmative	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	Michael Shaw		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Mike Smith		None	N/A
1	MEAG Power	David Weekley	Scott Miller	Affirmative	N/A
1	Memphis Light, Gas and Water Division	Allan Long		None	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Negative	Comments Submitted
1	Muscatine Power and Water	Andy Kurriger		Negative	Third-Party Comments
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Affirmative	N/A
1	Nebraska Public Power District	Jamison Cawley		Negative	Third-Party Comments
1	New York Power Authority	Salvatore Spagnolo		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Affirmative	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Affirmative	N/A
1	Northeast Missouri Electric Power Cooperative	Kevin White		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Negative	Third-Party Comments
1	Ohio Valley Electric Corporation	Scott Cunningham		Affirmative	N/A
1	Omaha Public Power District	Doug Peterchuck		Negative	Comments Submitted
1	Oncor Electric Delivery	Lee Maurer	Tho Tran	Negative	Comments Submitted
1	OTP - Otter Tail Power Company	Charles Wicklund		Negative	Third-Party Comments
1	Peak Reliability	Scott Downey		Affirmative	N/A
1	PNM Resources - Public Service Company of New Mexico	Laurie Williams		Affirmative	N/A
1	PPL Electric Utilities Corporation	Brenda Truhe		Affirmative	N/A
1	PSEG - Public Service Electric and Gas Co.	Joseph Smith		Affirmative	N/A
1	Public Utility District No. 1 of Chelan County	Jeff Kimbell		None	N/A
1	Public Utility District No. 1 of Snohomish County	Long Duong		Abstain	N/A
1	Puget Sound Energy, Inc.	Theresa Rakowsky		Affirmative	N/A
1	Sacramento Municipal Utility District	Arthur Starkovich	Joe Tarantino	Affirmative	N/A
1	Salt River Project	Steven Cobb		Negative	Comments Submitted
1	Santee Cooper	Chris Wagner		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	SCANA - South Carolina Electric and Gas Co.	Tom Hanzlik		Abstain	N/A
1	Seattle City Light	Pawel Krupa		None	N/A
1	Seminole Electric Cooperative, Inc.	Mark Churilla		None	N/A
1	Sempra - San Diego Gas and Electric	Martine Blair	Jeff Johnson	Affirmative	N/A
1	Sho-Me Power Electric Cooperative	Peter Dawson		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Katherine Prewitt		Affirmative	N/A
1	Southern Indiana Gas and Electric Co.	Steve Rawlinson		Affirmative	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell		None	N/A
1	Tennessee Valley Authority	Howell Scott		Affirmative	N/A
1	Tri-State G and T Association, Inc.	Tracy Sliman		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Negative	Comments Submitted
1	Westar Energy	Allen Klassen		Negative	Third-Party Comments
1	Western Area Power Administration	sean erickson		Negative	Third-Party Comments
1	Xcel Energy, Inc.	Dean Schiro		Affirmative	N/A
2	California ISO	Richard Vine		Abstain	N/A
2	Electric Reliability Council of Texas, Inc.	Brandon Gleason		Affirmative	N/A
2	Independent Electricity System Operator	Leonard Kula		Affirmative	N/A
2	ISO New England, Inc.	Michael Puscas		None	N/A
2	Midcontinent ISO, Inc.	Terry BIlke		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
2	New York Independent System Operator	Gregory Campoli		Affirmative	N/A
2	PJM Interconnection, L.L.C.	Mark Holman		Affirmative	N/A
3	AEP	Aaron Austin		Affirmative	N/A
3	AES - Indianapolis Power and Light Co.	Bette White		None	N/A
3	APS - Arizona Public Service Co.	Vivian Vo		Affirmative	N/A
3	Arkansas Electric Cooperative Corporation	Philip Huff		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	W. Dwayne Preston		Affirmative	N/A
3	Basin Electric Power Cooperative	Jeremy Voll		None	N/A
3	BC Hydro and Power Authority	Hootan Jarollahi		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Annette Johnston	Darnez Gresham	Affirmative	N/A
3	Bonneville Power Administration	Rebecca Berdahl		Negative	Comments Submitted
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City of Farmington	Linda Jacobson-Quinn		Abstain	N/A
3	City of Leesburg	Chris Adkins		None	N/A
3	City of Vero Beach	Ginny Beigel	Brandon McCormick	Negative	Comments Submitted
3	City Utilities of Springfield, Missouri	Scott Williams		None	N/A
3	Cleco Corporation	Michelle Corley	Louis Guidry	Negative	Third-Party Comments
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Cowlitz County PUD	Russell Noble		None	N/A
3	Duke Energy	Lee Schuster		Negative	Comments Submitted
3	Edison International - Southern California Edison Company	Romel Aquino		None	N/A
3	Empire District Electric Co.	Kalem Long		None	N/A
3	Eversource Energy	Sharon Flannery		Affirmative	N/A
3	Exelon	John Bee		Negative	Comments Submitted
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great Plains Energy - Kansas City Power and Light Co.	Jessica Tucker	Douglas Webb	Negative	Third-Party Comments
3	Great River Energy	Brian Glover		Negative	Third-Party Comments
3	Hydro One Networks, Inc.	Paul Malozewski		None	N/A
3	KAMO Electric Cooperative	Ted Hilmes		Affirmative	N/A
3	Lincoln Electric System	Jason Fortik		Negative	Third-Party Comments
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	Manitoba Hydro	Karim Abdel-Hadi		None	N/A
3	MEAG Power	Roger Brand	Scott Miller	Affirmative	N/A
3	Modesto Irrigation District	Jack Savage	Nick Braden	Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Negative	Third-Party Comments
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Negative	Third-Party Comments
3	New York Power Authority	David Rivera		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	NiSource - Northern Indiana Public Service Co.	Aimee Harris		Affirmative	N/A
3	North Carolina Electric Membership Corporation	doug white	Scott Brame	Affirmative	N/A
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Affirmative	N/A
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen		None	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Negative	Third-Party Comments
3	OTP - Otter Tail Power Company	Wendi Olson		Negative	Third-Party Comments
3	Owensboro Municipal Utilities	Thomas Lyons		Affirmative	N/A
3	Platte River Power Authority	Jeff Landis		Affirmative	N/A
3	PNM Resources - Public Service Company of New Mexico	Lynn Goldstein		Affirmative	N/A
3	Portland General Electric Co.	Angela Gaines		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	Charles Freibert		Affirmative	N/A
3	PSEG - Public Service Electric and Gas Co.	Jeffrey Mueller		Affirmative	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Abstain	N/A
3	Puget Sound Energy, Inc.	Lynda Kupfer		Affirmative	N/A
3	Rutherford EMC	Tom Haire		None	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Joe Tarantino	Affirmative	N/A
3	Salt River Project	Robert Kondziolka		Negative	Comments Submitted
3	Santee Cooper	James Poston		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	SCANA - South Carolina Electric and Gas Co.	Scott Parker		None	N/A
3	Seattle City Light	Tuan Tran		Affirmative	N/A
3	Seminole Electric Cooperative, Inc.	James Frauen		Abstain	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jeff Neas		Affirmative	N/A
3	Silicon Valley Power - City of Santa Clara	Val Ridad		None	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Abstain	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Fred Frederick		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson		None	N/A
3	TECO - Tampa Electric Co.	Ronald Donahey		None	N/A
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A
3	Tri-State G and T Association, Inc.	Janelle Marriott Gill		None	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Third-Party Comments
3	Westar Energy	Bryan Taggart		Negative	Third-Party Comments
3	Xcel Energy, Inc.	Michael Ibold		Affirmative	N/A
4	American Public Power Association	Jack Cashin		None	N/A
4	Arkansas Electric Cooperative Corporation	Alice Wright		Affirmative	N/A
4	Austin Energy	Esther Weekes		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	City of Clewiston	Lynne Mila	Brandon McCormick	Negative	Comments Submitted
4	City Utilities of Springfield, Missouri	John Allen		None	N/A
4	FirstEnergy - FirstEnergy Corporation	Aubrey Short		Affirmative	N/A
4	Georgia System Operations Corporation	Andrea Barclay		Affirmative	N/A
4	Indiana Municipal Power Agency	Jack Alvey	Scott Berry	None	N/A
4	National Rural Electric Cooperative Association	Barry Lawson		Affirmative	N/A
4	North Carolina Electric Membership Corporation	John Lemire	Scott Brame	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John Martinsen		Abstain	N/A
4	Sacramento Municipal Utility District	Beth Tincher	Joe Tarantino	Affirmative	N/A
4	Seattle City Light	Hao Li		Affirmative	N/A
4	Seminole Electric Cooperative, Inc.	Charles Wubbena		None	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho		None	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		None	N/A
4	WEC Energy Group, Inc.	Anthony Jankowski		Negative	Third-Party Comments
5	Acciona Energy North America	George Brown		None	N/A
5	AEP	Thomas Foltz		Affirmative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Negative	Comments Submitted
5	APS - Arizona Public Service Co.	Kelsi Rigby		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Arkansas Electric Cooperative Corporation	Moses Harris		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Brad Haralson		Affirmative	N/A
5	Austin Energy	Shirley Mathew		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		None	N/A
5	Basin Electric Power Cooperative	Mike Kraft		None	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Affirmative	N/A
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		Affirmative	N/A
5	Bonneville Power Administration	Scott Winner		Negative	Comments Submitted
5	BP Wind Energy North America Inc.	Carla Holly		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Affirmative	N/A
5	Cleco Corporation	Stephanie Huffman	Louis Guidry	Negative	Third-Party Comments
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Negative	Comments Submitted
5	Colorado Springs Utilities	Jeff Icke		None	N/A
5	Con Ed - Consolidated Edison Co. of New York	William Winters	Alyson Slanover	Affirmative	N/A
5	Dairyland Power Cooperative	Tommy Drea		None	N/A
5	Dominion - Dominion Resources, Inc.	Lou Oberski		None	N/A
5	Duke Energy	Dale Goodwine		Negative	Comments Submitted
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy	Jamie Prater		Affirmative	N/A
5	Exelon	Ruth Miller		Negative	Comments Submitted
5	FirstEnergy - FirstEnergy Solutions	Robert Loy		Affirmative	N/A
5	Great Plains Energy - Kansas City Power and Light Co.	Harold Wyble	Douglas Webb	Negative	Third-Party Comments
5	Great River Energy	Preston Walsh		Negative	Third-Party Comments
5	Gridforce Energy Management, LLC	David Blackshear		None	N/A
5	Hydro-Qu?bec Production	Junji Yamaguchi		None	N/A
5	JEA	John Babik		None	N/A
5	Kissimmee Utility Authority	Mike Blough	Brandon McCormick	Negative	Comments Submitted
5	Lakeland Electric	Jim Howard		Negative	Third-Party Comments
5	Lincoln Electric System	Kayleigh Wilkerson		Negative	Third-Party Comments
5	Los Angeles Department of Water and Power	Glenn Barry		None	N/A
5	Manitoba Hydro	Yuguang Xiao		None	N/A
5	Massachusetts Municipal Wholesale Electric Company	David Gordon		Affirmative	N/A
5	MEAG Power	Steven Grego	Scott Miller	Affirmative	N/A
5	Muscatine Power and Water	Neal Nelson		Negative	Third-Party Comments
5	NB Power Corporation	Laura McLeod		None	N/A
5	Nebraska Public Power District	Don Schmit		Negative	Third-Party Comments
5	New York Power Authority	Erick Barrios		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	NextEra Energy	Allen Schriver		Affirmative	N/A
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Affirmative	N/A
5	North Carolina Electric Membership Corporation	Robert Beadle	Scott Brame	Affirmative	N/A
5	Northern California Power Agency	Marty Hostler		Negative	Comments Submitted
5	OGE Energy - Oklahoma Gas and Electric Co.	John Rhea		Negative	Third-Party Comments
5	Omaha Public Power District	Mahmood Safi		Negative	Comments Submitted
5	Ontario Power Generation Inc.	David Ramkalawan		Affirmative	N/A
5	OTP - Otter Tail Power Company	Cathy Fogale		Negative	Third-Party Comments
5	Portland General Electric Co.	Ryan Olson		None	N/A
5	PPL - Louisville Gas and Electric Co.	JULIE HOSTRANDER		None	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Affirmative	N/A
5	Public Utility District No. 1 of Chelan County	Haley Sousa		Abstain	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Abstain	N/A
5	Puget Sound Energy, Inc.	Eleanor Ewry		Affirmative	N/A
5	Sacramento Municipal Utility District	Susan Oto	Joe Tarantino	Affirmative	N/A
5	Salt River Project	Kevin Nielsen		Negative	Comments Submitted
5	Santee Cooper	Tommy Curtis		Negative	Comments Submitted
5	SCANA - South Carolina Electric and Gas Co.	Alyssa Hubbard		None	N/A
5	Seattle City Light	Faz Kasraie		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Seminole Electric Cooperative, Inc.	Brenda Atkins		None	N/A
5	Sempra - San Diego Gas and Electric	Daniel Frank	Andrey Komissarov	None	N/A
5	Silicon Valley Power - City of Santa Clara	Sandra Pacheco		None	N/A
5	Southern Company - Southern Company Generation	William D. Shultz		Affirmative	N/A
5	SunPower	Bradley Collard		None	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin		None	N/A
5	Talen Generation, LLC	Matthew McMillan		None	N/A
5	TECO - Tampa Electric Co.	Frank L Busot		None	N/A
5	Tennessee Valley Authority	M Lee Thomas		Affirmative	N/A
5	U.S. Bureau of Reclamation	Wendy Center		Negative	Comments Submitted
5	WEC Energy Group, Inc.	Linda Horn		Negative	Third-Party Comments
5	Xcel Energy, Inc.	Gerry Huitt		Affirmative	N/A
6	APS - Arizona Public Service Co.	Jonathan Aragon		Affirmative	N/A
6	Arkansas Electric Cooperative Corporation	Bruce Walkup		Affirmative	N/A
6	Austin Energy	Andrew Gallo		Affirmative	N/A
6	Basin Electric Power Cooperative	Paul Huettl		None	N/A
6	Berkshire Hathaway - PacifiCorp	Sandra Shaffer		Affirmative	N/A
6	Bonneville Power Administration	Andrew Meyers		Negative	Comments Submitted
6	Cleco Corporation	Robert Hirchak	Louis Guidry	Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Con Ed - Consolidated Edison Co. of New York	Christopher Overberg		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Affirmative	N/A
6	Duke Energy	Greg Cecil		Negative	Comments Submitted
6	Edison International - Southern California Edison Company	Kenya Streeter		None	N/A
6	Entergy	Julie Hall		Affirmative	N/A
6	Exelon	Becky Webb		Negative	Comments Submitted
6	FirstEnergy - FirstEnergy Solutions	Ann Ivanc		Affirmative	N/A
6	Florida Municipal Power Pool	Tom Reedy	Brandon McCormick	Negative	Comments Submitted
6	Great Plains Energy - Kansas City Power and Light Co.	Jim Flucke	Douglas Webb	Negative	Third-Party Comments
6	Lincoln Electric System	Eric Ruskamp		Negative	Third-Party Comments
6	Los Angeles Department of Water and Power	Anton Vu		Affirmative	N/A
6	Luminant - Luminant Energy	Brenda Hampton		Abstain	N/A
6	Manitoba Hydro	Blair Mukanik		None	N/A
6	Modesto Irrigation District	James McFall	Nick Braden	Affirmative	N/A
6	Muscatine Power and Water	Ryan Streck		Negative	Third-Party Comments
6	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		None	N/A
6	NiSource - Northern Indiana Public Service Co.	Joe O'Brien		Affirmative	N/A
6	Northern California Power Agency	Dennis Sismaet		Negative	Comments Submitted
6	OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Omaha Public Power District	Joel Robles		None	N/A
6	Portland General Electric Co.	Daniel Mason		Affirmative	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
6	Public Utility District No. 1 of Chelan County	Davis Jelusich		Abstain	N/A
6	Public Utility District No. 2 of Grant County, Washington	LeRoy Patterson		None	N/A
6	Sacramento Municipal Utility District	Jamie Cutlip	Joe Tarantino	Affirmative	N/A
6	Salt River Project	Bobby Olsen		Negative	Comments Submitted
6	Santee Cooper	Michael Brown		Negative	Comments Submitted
6	Seattle City Light	Charles Freeman		Affirmative	N/A
6	Seminole Electric Cooperative, Inc.	Trudy Novak		Abstain	N/A
6	Snohomish County PUD No. 1	Franklin Lu		Abstain	N/A
6	Southern Company - Southern Company Generation and Energy Marketing	Jennifer Sykes		Affirmative	N/A
6	Southern Indiana Gas and Electric Co.	Brad Lisembee		None	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Rick Applegate		Abstain	N/A
6	Talen Energy Marketing, LLC	Jennifer Hohenshilt		None	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Affirmative	N/A
6	WEC Energy Group, Inc.	David Hathaway		Negative	Third-Party Comments
6	Westar Energy	Megan Wagner	Douglas Webb	Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Xcel Energy, Inc.	Carrie Dixon		Affirmative	N/A
7	Exxon Mobil	Jay Barnett		None	N/A
7	Luminant Mining Company LLC	Stewart Rake		Abstain	N/A
8	David Kiguel	David Kiguel		Affirmative	N/A
8	Massachusetts Attorney General	Frederick Plett		None	N/A
8	Roger Zaklukiewicz	Roger Zaklukiewicz		Affirmative	N/A
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson		Affirmative	N/A
10	Midwest Reliability Organization	Russel Mountjoy		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Affirmative	N/A
10	Northeast Power Coordinating Council	Guy V. Zito		Affirmative	N/A
10	ReliabilityFirst	Anthony Jablonski		Affirmative	N/A
10	SERC Reliability Corporation	Drew Slabaugh		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Negative	Comments Submitted
10	Western Electricity Coordinating Council	Steven Rueckert		Negative	Comments Submitted

Previous 1 Next

Showing 1 to 309 of 309 entries

BALLOT RESULTS

Ballot Name: 2016-02 Modifications to CIP Standards CIP-012-1 Non-binding Poll AB 4 NB
Voting Start Date: 6/22/2018 12:01:00 AM
Voting End Date: 7/5/2018 8:00:00 PM
Ballot Type: NB
Ballot Activity: AB
Ballot Series: 4
Total # Votes: 224
Total Ballot Pool: 290
Quorum: 77.24
Weighted Segment Value: 69.77

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 1	75	1	36	0.75	12	0.25	13	13
Segment: 2	7	0.3	3	0.3	0	0	3	1
Segment: 3	70	1	30	0.714	12	0.286	12	15
Segment: 4	14	0.8	6	0.6	2	0.2	1	5
Segment: 5	69	1	23	0.59	16	0.41	9	21
Segment: 6	42	1	14	0.583	10	0.417	9	9
Segment: 7	2	0	0	0	0	0	1	1
Segment: 8	3	0.2	2	0.2	0	0	0	1
Segment: 9	1	0.1	1	0.1	0	0	0	0
Segment: 10	7	0.5	5	0.5	0	0	2	0
Totals:	290	5.9	120	4.337	52	1.563	50	66

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Affirmative	N/A
1	American Transmission Company, LLC	Douglas Johnson		Affirmative	N/A
1	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	John Shaver		None	N/A
1	Associated Electric Cooperative, Inc.	Ryan Ziegler		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Joe Tarantino	Affirmative	N/A
1	Basin Electric Power Cooperative	David Rudolph		None	N/A
1	BC Hydro and Power Authority	Patricia Robertson		Abstain	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Bonneville Power Administration	Kammy Rogers-Holliday		Negative	Comments Submitted
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		Affirmative	N/A
1	Cedar Falls Utilities	Adam Peterson		None	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Hudson Gas & Electric Corp.	Frank Pace		Affirmative	N/A
1	City Utilities of Springfield, Missouri	Michael Buyce		None	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Larry Nash		Abstain	N/A
1	Duke Energy	Laura Lee		Negative	Comments Submitted
1	Edison International - Southern California Edison Company	Steven Mavis		Affirmative	N/A
1	Entergy - Entergy Services, Inc.	Oliver Burke		Affirmative	N/A
1	Eversource Energy	Quintin Lee		Affirmative	N/A
1	Exelon	Chris Scanlon		Abstain	N/A
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A
1	Great Plains Energy - Kansas City Power and Light Co.	James McBee	Douglas Webb	Negative	Comments Submitted
1	Great River Energy	Gordon Pietsch		None	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Affirmative	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Affirmative	N/A
1	IDACORP - Idaho Power Company	Laura Nelson		Abstain	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz		None	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Stephanie Burns	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Lincoln Electric System	Danny Pudenz		Abstain	N/A
1	Long Island Power Authority	Robert Ganley		Abstain	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		Affirmative	N/A
1	Lower Colorado River Authority	Michael Shaw		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Mike Smith		None	N/A
1	MEAG Power	David Weekley	Scott Miller	Affirmative	N/A
1	Memphis Light, Gas and Water Division	Allan Long		Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Negative	Comments Submitted
1	Muscatine Power and Water	Andy Kurriger		Negative	Comments Submitted
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Affirmative	N/A
1	Nebraska Public Power District	Jamison Cawley		Abstain	N/A
1	New York Power Authority	Salvatore Spagnolo		None	N/A
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Affirmative	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Affirmative	N/A
1	Northeast Missouri Electric Power Cooperative	Kevin White		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Negative	Comments Submitted
1	Ohio Valley Electric Corporation	Scott Cunningham		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Omaha Public Power District	Doug Peterchuck		Negative	Comments Submitted
1	OTP - Otter Tail Power Company	Charles Wicklund		Negative	Comments Submitted
1	Peak Reliability	Scott Downey		None	N/A
1	PNM Resources - Public Service Company of New Mexico	Laurie Williams		Affirmative	N/A
1	PPL Electric Utilities Corporation	Brenda Truhe		Abstain	N/A
1	PSEG - Public Service Electric and Gas Co.	Joseph Smith		Abstain	N/A
1	Public Utility District No. 1 of Chelan County	Jeff Kimbell		None	N/A
1	Public Utility District No. 1 of Snohomish County	Long Duong		Abstain	N/A
1	Puget Sound Energy, Inc.	Theresa Rakowsky		Affirmative	N/A
1	Sacramento Municipal Utility District	Arthur Starkovich	Joe Tarantino	Affirmative	N/A
1	Salt River Project	Steven Cobb		Negative	Comments Submitted
1	Santee Cooper	Chris Wagner		Abstain	N/A
1	SCANA - South Carolina Electric and Gas Co.	Tom Hanzlik		Abstain	N/A
1	Seattle City Light	Pawel Krupa		None	N/A
1	Seminole Electric Cooperative, Inc.	Mark Churilla		None	N/A
1	Sempra - San Diego Gas and Electric	Martine Blair	Jeff Johnson	Affirmative	N/A
1	Sho-Me Power Electric Cooperative	Peter Dawson		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Katherine Prewitt		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell		None	N/A
1	Tennessee Valley Authority	Howell Scott		Abstain	N/A
1	Tri-State G and T Association, Inc.	Tracy Sliman		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Negative	Comments Submitted
1	Westar Energy	Allen Klassen		Negative	No Comment Submitted
1	Western Area Power Administration	sean erickson		Negative	Comments Submitted
2	California ISO	Richard Vine		Abstain	N/A
2	Electric Reliability Council of Texas, Inc.	Brandon Gleason		Affirmative	N/A
2	Independent Electricity System Operator	Leonard Kula		Affirmative	N/A
2	ISO New England, Inc.	Michael Puscas		None	N/A
2	Midcontinent ISO, Inc.	Terry BIlke		Abstain	N/A
2	New York Independent System Operator	Gregory Campoli		Abstain	N/A
2	PJM Interconnection, L.L.C.	Mark Holman		Affirmative	N/A
3	AEP	Aaron Austin		Affirmative	N/A
3	AES - Indianapolis Power and Light Co.	Bette White		Affirmative	N/A
3	APS - Arizona Public Service Co.	Vivian Vo		Affirmative	N/A
3	Arkansas Electric Cooperative Corporation	Philip Huff		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	W. Dwayne Preston		Affirmative	N/A
3	Basin Electric Power Cooperative	Jeremy Voll		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Annette Johnston	Darnez Gresham	Affirmative	N/A
3	Bonneville Power Administration	Rebecca Berdahl		Negative	Comments Submitted
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City of Farmington	Linda Jacobson-Quinn		Abstain	N/A
3	City of Leesburg	Chris Adkins		None	N/A
3	City of Vero Beach	Ginny Beigel	Brandon McCormick	Negative	Comments Submitted
3	City Utilities of Springfield, Missouri	Scott Williams		None	N/A
3	Cleco Corporation	Michelle Corley	Louis Guidry	Negative	Comments Submitted
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
3	Cowlitz County PUD	Russell Noble		None	N/A
3	Duke Energy	Lee Schuster		Negative	Comments Submitted
3	Edison International - Southern California Edison Company	Romel Aquino		None	N/A
3	Eversource Energy	Sharon Flannery		Affirmative	N/A
3	Exelon	John Bee		Abstain	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great Plains Energy - Kansas City Power and Light Co.	Jessica Tucker	Douglas Webb	Negative	Comments Submitted
3	Great River Energy	Brian Glover		Negative	Comments Submitted
3	Hydro One Networks, Inc.	Paul Malozewski		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	KAMO Electric Cooperative	Ted Hilmes		Affirmative	N/A
3	Lincoln Electric System	Jason Fortik		Abstain	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	Manitoba Hydro	Karim Abdel-Hadi		None	N/A
3	MEAG Power	Roger Brand	Scott Miller	Affirmative	N/A
3	Modesto Irrigation District	Jack Savage	Nick Braden	Abstain	N/A
3	Muscatine Power and Water	Seth Shoemaker		Negative	Comments Submitted
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Abstain	N/A
3	New York Power Authority	David Rivera		None	N/A
3	NiSource - Northern Indiana Public Service Co.	Aimee Harris		Affirmative	N/A
3	North Carolina Electric Membership Corporation	doug white	Scott Brame	Affirmative	N/A
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Affirmative	N/A
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
3	Ocala Utility Services	Randy Hahn		Negative	Comments Submitted
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Negative	Comments Submitted
3	OTP - Otter Tail Power Company	Wendi Olson		Negative	Comments Submitted
3	Owensboro Municipal Utilities	Thomas Lyons		Affirmative	N/A
3	Platte River Power Authority	Jeff Landis		Affirmative	N/A
3	PNM Resources - Public Service Company of New Mexico	Lynn Goldstein		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Portland General Electric Co.	Angela Gaines		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	Charles Freibert		None	N/A
3	PSEG - Public Service Electric and Gas Co.	Jeffrey Mueller		Abstain	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Abstain	N/A
3	Puget Sound Energy, Inc.	Lynda Kupfer		Affirmative	N/A
3	Rutherford EMC	Tom Haire		None	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Joe Tarantino	Affirmative	N/A
3	Salt River Project	Robert Kondziolka		Negative	Comments Submitted
3	Santee Cooper	James Poston		Abstain	N/A
3	SCANA - South Carolina Electric and Gas Co.	Scott Parker		None	N/A
3	Seattle City Light	Tuan Tran		Affirmative	N/A
3	Seminole Electric Cooperative, Inc.	James Frauen		Abstain	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jeff Neas		Affirmative	N/A
3	Silicon Valley Power - City of Santa Clara	Val Ridad		None	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Abstain	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson		None	N/A
3	TECO - Tampa Electric Co.	Ronald Donahey		None	N/A
3	Tennessee Valley Authority	Ian Grant		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Tri-State G and T Association, Inc.	Janelle Marriott Gill		None	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Comments Submitted
3	Westar Energy	Bryan Taggart		Negative	No Comment Submitted
3	Xcel Energy, Inc.	Michael Ibold		Abstain	N/A
4	American Public Power Association	Jack Cashin		None	N/A
4	Austin Energy	Esther Weekes		Affirmative	N/A
4	City of Clewiston	Lynne Mila	Brandon McCormick	Negative	Comments Submitted
4	City Utilities of Springfield, Missouri	John Allen		Affirmative	N/A
4	Georgia System Operations Corporation	Andrea Barclay		Affirmative	N/A
4	Indiana Municipal Power Agency	Jack Alvey	Scott Berry	None	N/A
4	North Carolina Electric Membership Corporation	John Lemire	Scott Brame	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John Martinsen		Abstain	N/A
4	Sacramento Municipal Utility District	Beth Tincher	Joe Tarantino	Affirmative	N/A
4	Seattle City Light	Hao Li		Affirmative	N/A
4	Seminole Electric Cooperative, Inc.	Charles Wubbena		None	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho		None	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		None	N/A
4	WEC Energy Group, Inc.	Anthony Jankowski		Negative	Comments Submitted
5	Acciona Energy North America	George Brown		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	AEP	Thomas Foltz		Affirmative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Affirmative	N/A
5	APS - Arizona Public Service Co.	Kelsi Rigby		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Brad Haralson		Affirmative	N/A
5	Austin Energy	Shirley Mathew		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		None	N/A
5	Basin Electric Power Cooperative	Mike Kraft		None	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Abstain	N/A
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		Affirmative	N/A
5	Bonneville Power Administration	Scott Winner		Negative	Comments Submitted
5	BP Wind Energy North America Inc.	Carla Holly		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Affirmative	N/A
5	Cleco Corporation	Stephanie Huffman	Louis Guidry	Negative	Comments Submitted
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Negative	Comments Submitted
5	Colorado Springs Utilities	Jeff Icke		None	N/A
5	Con Ed - Consolidated Edison Co. of New York	William Winters	Alyson Slanover	Affirmative	N/A
5	Dairyland Power Cooperative	Tommy Drea		None	N/A
5	Dominion - Dominion Resources, Inc.	Lou Oberski		None	N/A
5	Duke Energy	Dale Goodwine		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy	Jamie Prater		Affirmative	N/A
5	Exelon	Ruth Miller		Abstain	N/A
5	FirstEnergy - FirstEnergy Solutions	Robert Loy		Affirmative	N/A
5	Great Plains Energy - Kansas City Power and Light Co.	Harold Wyble	Douglas Webb	Negative	Comments Submitted
5	Great River Energy	Preston Walsh		Negative	Comments Submitted
5	Hydro-Qu?bec Production	Junji Yamaguchi		None	N/A
5	JEA	John Babik		Affirmative	N/A
5	Kissimmee Utility Authority	Mike Blough	Brandon McCormick	Negative	Comments Submitted
5	Lakeland Electric	Jim Howard		Negative	Comments Submitted
5	Lincoln Electric System	Kayleigh Wilkerson		Abstain	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		None	N/A
5	Manitoba Hydro	Yuguang Xiao		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	David Gordon		Affirmative	N/A
5	MEAG Power	Steven Grego	Scott Miller	Affirmative	N/A
5	Muscatine Power and Water	Neal Nelson		Negative	Comments Submitted
5	NB Power Corporation	Laura McLeod		Abstain	N/A
5	Nebraska Public Power District	Don Schmit		Abstain	N/A
5	New York Power Authority	Erick Barrios		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	NextEra Energy	Allen Schriver		Affirmative	N/A
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Affirmative	N/A
5	Northern California Power Agency	Marty Hostler		Negative	Comments Submitted
5	OGE Energy - Oklahoma Gas and Electric Co.	John Rhea		Negative	Comments Submitted
5	Omaha Public Power District	Mahmood Safi		Negative	Comments Submitted
5	Ontario Power Generation Inc.	David Ramkalawan		Affirmative	N/A
5	OTP - Otter Tail Power Company	Cathy Fogale		Negative	Comments Submitted
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	JULIE HOSTRANDER		None	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A
5	Public Utility District No. 1 of Chelan County	Haley Sousa		Abstain	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Abstain	N/A
5	Puget Sound Energy, Inc.	Eleanor Ewry		Affirmative	N/A
5	Sacramento Municipal Utility District	Susan Oto	Joe Tarantino	Affirmative	N/A
5	Salt River Project	Kevin Nielsen		Negative	Comments Submitted
5	Santee Cooper	Tommy Curtis		Abstain	N/A
5	SCANA - South Carolina Electric and Gas Co.	Alyssa Hubbard		None	N/A
5	Seattle City Light	Faz Kasraie		None	N/A
5	Seminole Electric Cooperative, Inc.	Brenda Atkins		None	N/A
5	Sempra - San Diego Gas and Electric	Daniel Frank	Andrey Komissarov	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Silicon Valley Power - City of Santa Clara	Sandra Pacheco		None	N/A
5	Southern Company - Southern Company Generation	William D. Shultz		Affirmative	N/A
5	SunPower	Bradley Collard		None	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin		None	N/A
5	Talen Generation, LLC	Matthew McMillan		None	N/A
5	TECO - Tampa Electric Co.	Frank L Busot		None	N/A
5	Tennessee Valley Authority	M Lee Thomas		None	N/A
5	U.S. Bureau of Reclamation	Wendy Center		Negative	Comments Submitted
5	Westar Energy	Laura Cox	Douglas Webb	Negative	Comments Submitted
6	APS - Arizona Public Service Co.	Jonathan Aragon		Affirmative	N/A
6	Arkansas Electric Cooperative Corporation	Bruce Walkup		Affirmative	N/A
6	Austin Energy	Andrew Gallo		Affirmative	N/A
6	Basin Electric Power Cooperative	Paul Huettl		None	N/A
6	Berkshire Hathaway - PacifiCorp	Sandra Shaffer		Affirmative	N/A
6	Cleco Corporation	Robert Hirchak	Louis Guidry	Negative	Comments Submitted
6	Con Ed - Consolidated Edison Co. of New York	Christopher Overberg		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Affirmative	N/A
6	Duke Energy	Greg Cecil		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Edison International - Southern California Edison Company	Kenya Streeter		None	N/A
6	Entergy	Julie Hall		Affirmative	N/A
6	Exelon	Becky Webb		Abstain	N/A
6	FirstEnergy - FirstEnergy Solutions	Ann Ivanc		Affirmative	N/A
6	Florida Municipal Power Pool	Tom Reedy	Brandon McCormick	Negative	Comments Submitted
6	Great Plains Energy - Kansas City Power and Light Co.	Jim Flucke	Douglas Webb	Negative	Comments Submitted
6	Lincoln Electric System	Eric Ruskamp		Abstain	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Affirmative	N/A
6	Luminant - Luminant Energy	Brenda Hampton		Abstain	N/A
6	Manitoba Hydro	Blair Mukanik		None	N/A
6	Muscatine Power and Water	Ryan Streck		Negative	Comments Submitted
6	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		None	N/A
6	NiSource - Northern Indiana Public Service Co.	Joe O'Brien		Affirmative	N/A
6	Northern California Power Agency	Dennis Sismaet		Negative	Comments Submitted
6	OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay		Negative	Comments Submitted
6	Omaha Public Power District	Joel Robles		None	N/A
6	Portland General Electric Co.	Daniel Mason		Affirmative	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		None	N/A
6	Public Utility District No. 1 of Chelan County	Davis Jelusich		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Public Utility District No. 2 of Grant County, Washington	LeRoy Patterson		None	N/A
6	Sacramento Municipal Utility District	Jamie Cutlip	Joe Tarantino	Affirmative	N/A
6	Salt River Project	Bobby Olsen		Negative	Comments Submitted
6	Santee Cooper	Michael Brown		Abstain	N/A
6	Seattle City Light	Charles Freeman		Affirmative	N/A
6	Seminole Electric Cooperative, Inc.	Trudy Novak		Abstain	N/A
6	Snohomish County PUD No. 1	Franklin Lu		Abstain	N/A
6	Southern Company - Southern Company Generation and Energy Marketing	Jennifer Sykes		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Rick Applegate		Abstain	N/A
6	Talen Energy Marketing, LLC	Jennifer Hohenshilt		None	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Abstain	N/A
6	WEC Energy Group, Inc.	David Hathaway		Negative	Comments Submitted
6	Westar Energy	Megan Wagner	Douglas Webb	Negative	Comments Submitted
7	Exxon Mobil	Jay Barnett		None	N/A
7	Luminant Mining Company LLC	Stewart Rake		Abstain	N/A
8	David Kiguel	David Kiguel		Affirmative	N/A
8	Massachusetts Attorney General	Frederick Plett		None	N/A
8	Roger Zaklukiewicz	Roger Zaklukiewicz		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson		Affirmative	N/A
10	Midwest Reliability Organization	Russel Mountjoy		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Affirmative	N/A
10	Northeast Power Coordinating Council	Guy V. Zito		Affirmative	N/A
10	ReliabilityFirst	Anthony Jablonski		Affirmative	N/A
10	SERC Reliability Corporation	Drew Slabaugh		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Abstain	N/A

Previous 1 Next

Showing 1 to 290 of 290 entries

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP-012-1

Project 2016-02 Modifications to the CIP Standards: Consideration of Comments

August 2018

RELIABILITY | ACCOUNTABILITY



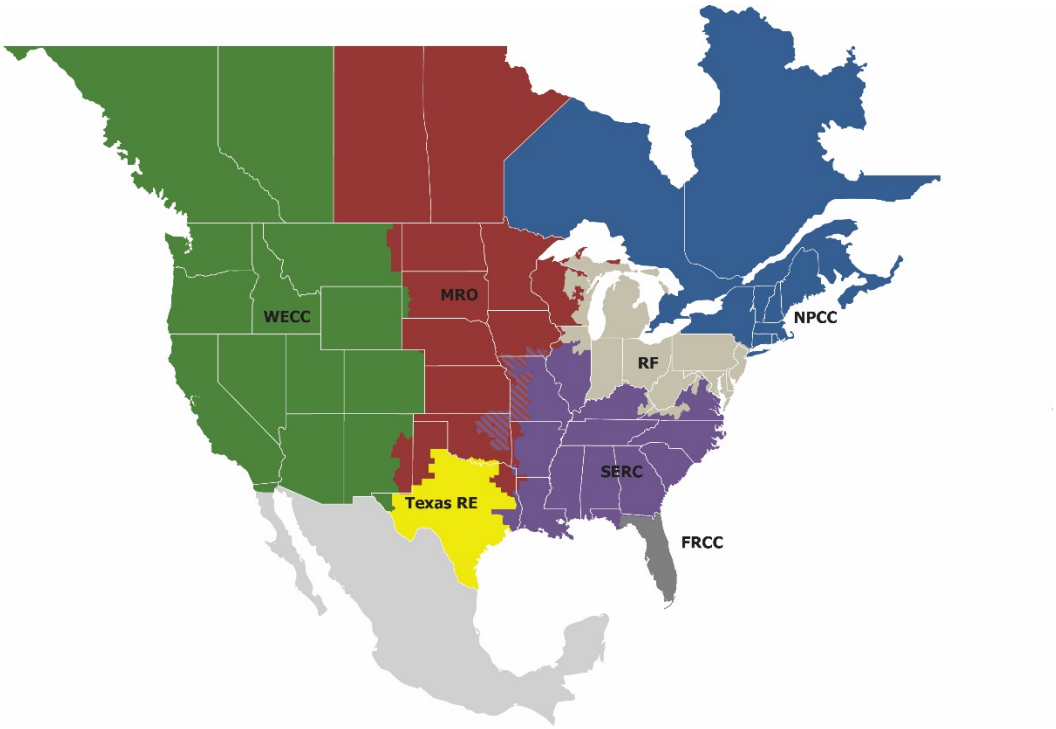

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Preface

The vision for the Electric Reliability Organization (ERO) Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the seven Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

The North American BPS is divided into seven RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.



FRCC	Florida Reliability Coordinating Council
MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

Background

The Project 2016-02 Modifications to CIP Standards Drafting Team thanks all commenters who submitted comments on the draft CIP-012-1 standard. This standard was posted for a 45-day public comment period through Friday, April 30, 2018. Stakeholders were asked to provide feedback on the standards and associated documents through a special electronic comment form. There were 58 sets of responses, including comments from approximately 155 different people from approximately 108 companies representing the 10 Industry Segments as shown in the table on the following pages.

All comments submitted may be reviewed in their original format on the standard's project page.

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process. If you feel there has been an error or omission, you can contact the NERC standards developer, Jordan Mallory, at 404-446-2589 or at jordan.mallory@nerc.net.

CIP-012-1 Consideration of Comments

Purpose

The Modification to CIP Standards drafting team appreciates industry's comments on the CIP-012-1 standard. The SDT reviewed all comments carefully and made changes to the standard accordingly. The following pages are a summary of the comments received and how the CIP SDT addressed them. If a specific comment was not addressed in the summary of comments, please contact the NERC standards developer.

Control Center Definition

Many commenters expressed concern with the proposed Control Center definition.

The SDT decided to draft exemption language within the applicability section of CIP-012 instead of revising the Control Center definition. Please see the Control Center definition consideration of comments report for additional SDT responses on the new path taken by the SDT.

Control Center

A commenter suggested that the SDT is compounding the Control Center issue by having another explanation of a Control Center/control center to those already present in CIP-002, CIP-014, and the NERC Glossary, and now CIP-012. We recommend a single document that explains the Control Center / control center topic.

The SDT is using this Technical Rationale document to explain its intent in developing the exclusion language in CIP-012-1. The exclusion in CIP-012 is for communications between certain Control Centers and does not modify the definition of Control Center. Use of the Control Center term in other standards is not within the scope of this SDT's SAR.

Control Center Exemption Language

Some commenters provided various examples of language for clarity of the Control Center exemption language within CIP-012. One example of the suggested language and the SDTs response is:

4.2.3 A generating station, Transmission station or substation that is also a Control Center, but meets one of the following criteria:

4.2.3.1 Aggregates and transmits Real-time Assessment and Real-time monitoring data from two or more Generation resource(s), Transmission station(s) and/or substation(s) but all aggregated data comes from locations that are contained within the same physical perimeter. (see Figure 1)

4.2.3.2 The Control Center does not aggregate and transmit Real-time Assessment and Real-time monitoring data from location(s) outside the physical perimeter where it resides. (see Figure 2)

The SDT appreciates the included diagrams with Figure 1 and 2 to explain the intent. The SDT asserts that in Figure 1 if an entity defines station at a granular level to where multiple stations are in one "Facility Yard", this would still be considered one "location" and would not fall under the "two or more locations" attribute of the Control Center definition. Since the definition of Control Center uses the term "location", the SDT does not want to introduce a synonymous term of "physical perimeter" and considers the two equivalent.

The SDT also agrees with the scenario depicted in Figure 2. In this scenario, Station 1 could be considered a Control Center depending on the functionality available through the communications to the dual-ported RTUs at other locations. Assuming each separate location is reporting its data to the TOP Control Center with its own individual RTU, that communication is exempted from CIP-012.

Based on these comments, the SDT has created a similar diagram to the ones provided and included it in the Technical Rationale document.

Some commenters recommended the below change along with rationale drafted explaining the reason for the exemption.

A Control Center at a BES generation resource or Transmission station or substation that transmits to another Control Center Real-time Assessment or Real-time monitoring data, such as RTU-style data, pertaining only to the generation resource or Transmission station or substation at which the data transmitting transmitted Control Center is located.

Rationale: The first use of "Control Center" implies that the exemption is for a Control Center to start with. Where it is not a Control Center but a BES facility that transmits data, via an RTU (RTU was added since it plays a pivotal point of intent within the Technical Rational document).

The SDT modified the Technical Rationale document explaining the reason for the Control Center exemption. In addition to the clarifying changes to the Control Center exemption, please see the updated redline that provides clarifying changes in attempt to make the exemption clearer.

A commenter suggests that there could be increases in security risk with repair personnel going into a PSP without knowing all the CIP security requirements for such devices and have in-house personnel escorting the repair personnel during any repair work.

The SDT asserts that such risks are covered under other CIP standards such as CIP-006 and CIP-004.

Requirement R1

A commenter expressed that Real-time Assessments list a number of specific inputs that should be considered for both "Real-time Assessment (RTA) and Real-time monitoring (RTm) data." The commenter suggested there may be an audit approach taken that would require consideration of both RTA AND RTm data for proof that an entity provided adequate protections. The commenter requested that the SDT provide clarification on whether there is a distinction between data used for the RTA and data used for RTm. The commenter recommended consideration of the use of the inputs in the RTA NERC term with a caveat that Entities may choose to protect additional data if they feel the need to expand the scope.

The SDT relied on IRO-010-2 Requirement 1 and TOP-003-3 Requirement R1 that requires RCs, BAs, and TOPs to identify data used for RTA and RTm. The SDT stated in the Implementation Guidance that entities may choose to protect the data, the communication links, or both. The intent is that it may often be easier to identity the communication links over which two Control Centers exchange RTA and RTm data (as well as other data) and protect those communication links which protect all data flowing over them.

Some commenters questioned if CIP Exceptional Circumstance language needed to be added CIP-012-1.

The CIP Exceptional Circumstance language has been added to CIP-012.

A commenter expressed that "security protection used to mitigate risk" is too ambiguous. The commenter requested the SDT consider including two concepts in Requirement R1. The first concept is to clarify whether currently in place ICCP should be encrypted. The commenter noted that the requirement states "while being transmitted between any Control Centers." The commenter further noted that the draft Implementation Guidance has content talking about "both ends of the link" but did not include the expectations for the data while on the

link. The commenter was concerned with latency (primarily for generation control) if secure encryption is expected over the ICCP. Second concept is to include examples that include but are not limiting for security protection.

The SDT asserts that defining a plan to mitigate the risk of modification and disclosure of applicable data allows the Responsible Entity to document the processes that are supportable within its organization and offers flexibility in methods to meet the security objective. The SDT notes that the Implementation Guidance document offers examples of how to comply with the standard.

The SDT encourages Responsible Entities to submit additional scenarios as Implementation Guidance[1] through pre-qualified organizations for endorsement consideration.

Some commenters expressed that CIP-012 is unnecessary and that IRO-010 and TOP-003 already require a mutually agreeable security protocol. Additionally, another commenter expressed concern about the overlap between CIP-012 and TOP-003-3/IRO-010-2. The commenter questioned whether these standards should be combined.

FERC Order No. 822 paragraph 60 recognizes those requirements in IRO-010 and TOP-003 and states the reliability gap to be addressed as "while responsible entities are required to exchange real-time and operational planning data necessary to operate the bulk electric system using mutually agreeable security protocols, there is no technical specification for how this transfer of information should incorporate mandatory security controls." The modification of these other standards to remove the mutually agreeable security protocol requirement is outside the scope of this team's SAR.

A commenter requested clarity on the Responsible Entity in charge of securing the data being transmitted from a generator on RC, BA, and TOP equipment. The commenter suggested that the RC, BA, and TOP identify the GOP responsibilities under Part 1.3.

If the Generator is not a Control Center then CIP-012 does not apply as it is only between Control Centers. However, if the Generator is an applicable Control Center, then Requirement R1 Part 1.3 is intended to require the entities to document their responsibilities.

A commenter requested the SDT clarify whether CIP-012-1 applies to low, medium, or high BES Cyber Systems. The commenter requested the SDT also consider how to incorporate the scoping criteria into CIP-002.

The SDT asserts that the applicability is to data being transmitted between Control Centers of all impact levels in response to FERC Order 822 paragraph 58.

Some commenters noted that Real-time monitoring is not a defined term and that the R in Real-time should not be capitalized. In addition, the commenters expressed concern that coordination between Control Centers may result in compromises that may not satisfy the needs of the entities involved.

The term "Monitor" has been lowercased. "Real-time" is defined in the NERC Glossary of Terms and correctly used.

A commenter expressed concern that Operations Planning Analysis (OPA) data is not included in CIP-012-1. In addition, the commenter also noticed the Violation Time Horizon is for Operations Planning. Since the SDT has indicated reasons for excluding OPA data, the commenter asked whether the relevant Violation Time Horizon should be Real-time Operation.

[1] NERC Compliance Guidance Policy: https://www.nerc.com/pa/comp/guidance/Documents/Pre-qualified_org_submittal_with_form.pdf

Please see CIP-012-1 Consideration of Comments Summary Response for the OPA part. Due to the plan being drafted ahead of time; it would not be considered a Real-time Horizon and should remain operations planning horizon.

A commenter disagreed that having a plan adds to the reliability of protecting data used for Real-time Assessment and Real-time monitoring and commented that a plan is not needed. Some commenters recommended replacing the term "plan" with "process" throughout CIP-012-1, the Technical Rationale, Implementation Guidance, and other associated documents. Additionally, some commenters recommended that entities not be required to have a plan in Requirement R1, but have an actionable Requirement to implement. A suggestion was provided.

Based on industry feedback from a prior comment period, the SDT chose a requirement structure that is consistent with many other CIP standards to implement a documented plan. With regard to the use of the "process" instead of "plan", the SDT notes that the term 'documented process' refers to a set of required instructions specific to the Responsible Entity, designed to achieve a specific outcome. The plan to meet R1 may simply include documentation of the required elements of the Parts of CIP-012-1 Requirement R1. The plan also allows for R1 Part 1.3 to document the entities' responsibilities.

A commenter asked whether the current set of standards address those additional vulnerabilities in the entity's IT Security Plan. The commenter suggested that the current plan should be updated to include these additional risks, threats and integrated solution(s) that are already performed by the entity.

The documented plan(s) will need to address the security protection in place to mitigate the risk of unauthorized disclosure and unauthorized modification of applicable data transmitted between any Control Centers in accordance with the specified attributes in the Requirement Parts.

Some commenters questioned whether Requirement 1 Part 1.3 is needed.

Requirement R1 Part 1.3 provides entities a mechanism to specify which entity is responsible for the application of security controls, but not the actual security controls the other entity is responsible for. The SDT believes this is necessary for validation in an audit for an entity to have documented which controls it is responsible for in order to prevent the simultaneous auditing of multiple entities for each communication link between Control Centers operated by different Responsible Entities. Additionally, where data is transmitted between different entities, the SDT asserts that it is necessary for both entities to understand the responsibilities of applying the security controls for the entire transmission in order to ensure that the data is protected. Additional information has been added to the technical rationale document.

Some entities requested additional guidance around the different approaches to mitigating the risk of unauthorized disclosure or modification of data in transit.

The SDT encourages entities to work with prequalified organizations to submit Implementation Guidance for consideration.

A commenter asked if Real-time Data was operational data.

The term Real-time monitoring data was chosen for consistency with the data specification in TOP-003 and IRO-010 standards.

A commenter noted that the "SDT is not specifying the controls used to protect confidentiality and integrity. However, the only method available to achieve the proposed required objective is to implement encryption. FERC Order 822 states on page 39, "it is reasonable to conclude that any lag in communication speed resulting from implementation of protections [encryption technologies] should only be measureable on the order of milliseconds

and, therefore, will not adversely impact Control Center communications," but a commenter asserts this statement only refers to a single data stream. It is unknown what encryption will do when dealing with multiple data streams being transmitted at once, from one to many points, not only to the latency added for the reliable operation of the BES, but also to the computing resources."

The SDT agrees that encryption is a way to mitigate the identified risk and will be widely used as the method to do so, but does not want to be prescriptive due to new and improved technology in the future. The objective is to mitigate the identified risk and may require capacity updates to infrastructure in order to do so.

A commenter requested examples be provided on what a CIP exceptional circumstance would be.

The SDT's intent for including CIP Exceptional Circumstances within CIP-012 is to allow for scenarios where, for reliability reasons, restoration of availability of the data flowing between Control Centers may need to take precedence over temporarily unavailable security controls. For example, if two Control Centers are using encryption that is offloaded onto hardware cards and that encryption hardware fails, or if a key management system fails and numerous entities lose communication, the entities may need to restore the data flow as soon as possible for reliability purposes even if the encryption cannot be restored at the same time.

Implementation Plan

Some commenters stated that the 24-month timeline is not enough and requested the implementation timeline be increased to 36 months or a phased-in approach. Additionally, a commenter acknowledged that the standard and implementation plan are silent on physical security for the equipment being used to provide the data protection. The commenter provided an example of protection for a router that is located in another Entity's facility.

The SDT lengthened the implementation timeline in previous drafts based on industry input, but 24 months has met with widespread industry approval in later comment periods. The SDT concluded that a twenty-four (24) month implementation period is appropriate.

Some commenters noted the difficulty on providing responses to the implementation timeline until the Control Center definition is developed.

The SDT understands the uncertainty associated with CIP-012 if the Control Center definition is also under modification. The SDT attempted to modify the Control Center definition to handle issues brought about by CIP-012's communication scope but based on industry comments has chosen to address those specific communication concerns through an exemption in CIP-012. The Control Center definition remains stable. Please see the Consideration of Comments for the Control Center definition for additional information on the SDT's approach.

Technical Rationale for CIP-012-1

Some entities requested the SDT consider including some statements in the Technical Rationale to address the possibility that data requests made related to TOP-003 and/or IRO-010 include other data that is not Real-time Assessment data or Real-time monitoring data and how the Responsible Entity could exclude this other data from the security requirements.

The SDT agrees and has added a section on this topic to the Technical Rationale document.

A commenter noted that when addressing the security protections, the rationale should include that logical and physical controls can be used. The commenter suggested this should include the team's rationale for allowing these alternatives.

The SDT asserts that the Technical Rationale document already specifies that logical or physical controls can be used to achieve the required security objective.

A commenter noted that the number of regions needs to be updated.

The number of Regions has been updated to reflect the correct number.

Some commenters noted grammatical modifications:

- **In requirement R1 of the technical rationale document, the document should state document plan**
- **The alignment with IRO and TOP standards: last sentence "Real-time Monitoring ", the M should not be capitalized as it is not a NERC defined term.**
- **There appears to be a typo in the footer as it shows Reliability Standard CIP-002-1, instead of CIP-012-1**

The SDT agrees and has made the modifications as noted.

A commenter suggested a clarifying addition to the diagram on page 3 (Control Centers in Scope) of the Technical Rationale document: "In order to make the diagram more closely align to the statement made on page 8 of the Implementation Guidance which states:

'Entity Alpha does not need to consider any communications to other non-Control Center facilities such as generating plants or substations. These communications are out of scope for CIP-012-1.'

The statement above indicates that communications from a Control Center, to a non-Control Center (generation or sub) are out of scope. We suggest that a dotted line be added to the diagram on page 3 (Control Centers in Scope) of the Technical Rational and Justification document to show that communications from a GOP Control Center to a GOP Control Room should be considered out of scope. It is possible that a scenario could exist where GOP Control Centers pass information through a GOP Control Room out to Field Assets."

The SDT asserts that the diagram clearly shows the communications that are in and out of scope. Additionally, this diagram is simply one example and is not inclusive of all possible communication scenarios.

A commenter noted that adding control to the statement "Real-time monitoring" from TOP-003 and IRO-010 may set an expectation that control data will be part of those standards by default. The commenter noted that the proposed CIP-012-1 Implementation Guidance does not use "and control." The commenter recommended that if control is to be part of "Real-time monitoring" then the SDT should make the modifications to all documents, including the Glossary, to reduce misunderstanding.

Based on comments from the prior ballot and comment period, the SDT removed "and control" from the requirement for this posting. The SDT notes that the systems that provide control are generally the same systems that provide monitoring. The SDT removed "and control" to be consistent with the TOP-003 and IRO-010 standards.

A commenter requested that the SDT be consistent with other CIP standards and suggested the SDT combine the Technical Rationale document with the Implementation Guidance document within the draft standard. The commenter also requested the SDT clarify that CIP-012 is a standalone standard that is not associated with all the other CIP standards.

The Technical Rationale document and Implementation Guidance document serve two different purposes. The Technical Rationale document provides the SDT's intent and technical basis for the language in the standard. In

addition, the Technical Rationale document provides examples and diagrams to assist entities in understanding the language of the standard. Implementation Guidance is a means for registered entities to develop examples or approaches for ERO Enterprise endorsement to illustrate how registered entities could comply with a standard[2]. There is a project underway reviewing all of the current Technical Rationale documents and removing compliance examples from each document to submit for ERO Enterprise endorsement. Therefore, the Technical Rationale document and Implementation Guidance document cannot be merged together. While the applicability is different from other CIP standards, CIP-012-1 is one standard within the CIP Standard family.

A commenter expressed concern regarding the BCAs and EACMS used for CIP-012-1 may be considered out of scope for the rest of the CIP Reliability Standards based on a statement on Page 6: "The SDT also recognizes that CIP-012 security protection may be applied to a Cyber Asset that is not an identified BES Cyber Asset or EACMS. The identification of the Cyber Asset as the location where security protection is applied does not expand the scope of Cyber Assets identified as applicable under the CIP Cyber Security Standards CIP-002 through CIP-011."

The SDT notes that the assets where the security protection is applied under CIP-012 may be in data transport or telecom equipment that is between discrete ESPs and meet the exclusion in the CIP standards, but still be physically within a Control Center and thus meet the intent of protecting the data while being transmitted between Control Centers. CIP-012-1 neither expands nor diminishes the scope of applicable Cyber Assets under CIP-002 through CIP-011.

Some commenters noted difficulty with implementing Secure ICCP in the past because of concerns over the inability to guarantee a valid certificate at all times.

The SDT asserts that Secure ICCP is an option, but is one option to meeting the objective. The SDT included the flexibility to meet the objective and mitigate the risk at the application, network, or transport layers or even with physical security. Entities are allowed the implementation of physical or logical controls that best meet their operational and reliability needs as long as it meets the security objective specified in CIP-012-1 Requirement R1.

A commenter requested that the SDT provide additional information and a diagram for the scope and exemptions for SCADA data from multiple substations to a remote computer room where data is aggregated at the remote computer room prior to transmitting to a data center that is associated with the Operations Center.

The SDT asserts that CIP-012 provides for the protection of data while being transmitted between Control Centers only and thus excludes communications between Control Centers and field sites such as substations (FERC Order 822, paragraph 57).

A commenter suggested that the SDT provide examples in the Technical Rationale under what circumstances a generating resource or Transmission sub would be applicable to this standard.

The SDT asserts that the standard only applies to generation resources and Transmission substations when those facilities also meet the definition of a Control Center. In all other cases, the standard does not apply to such facilities.

Implementation Guidance

A commenter mentioned that when addressing the security protection that can be used in meeting CIP-012, examples of physical protection should be included in guidance. This should include details on how they can be used to address various parts of the communication between Control Centers.

[2] NERC Compliance Guidance Policy: https://www.nerc.com/pa/comp/guidance/Documents/Pre-qualified_org_submittal_with_form.pdf

The SDT has addressed an example within the implementation guidance document that includes physical protections. Typically physical protection might be used to protect communication links where encryption terminates at a device outside the Control Center in order to protect the data until it arrives inside the Control Center.

A commenter suggested that the last paragraph under Identification of where security protection is applied by the Responsible Entity be split into two separate paragraphs. The commenter suggested the first paragraph would describe how to handle "when exchanging data between two entities" and the second paragraph would focus on "when a Responsible Entity owns and operates both Control Centers."

The SDT agrees with the comment and split the paragraph into two separate paragraphs.

A commenter mentioned that the guidance document is good but until an entity does actual implementation and experiences any issues that arise from the implementation of CIP-012 requirement one can only assume the outcome.

The SDT notes there are a number of ways to demonstrate compliance with the requirement and encourages entities to develop and submit additional examples of Implementation Guidance through pre-qualified organizations for endorsement consideration.

A commenter stated that the implementation of R1.3 will require a standardized solution/technology between entities and a hierarchy of entity responsibilities. The commenter recommended the SDT add guidance and a requirement to identify the entity who is the controlling authority for the secure communications between two or more entities.

The SDT agrees that there will be coordination necessary and designed R1.3 to have the involved entities document those responsibilities. The requirement has been written to allow flexibility on how entities work together on this requirement. The SDT notes there are a number of ways to demonstrate compliance with the requirement and encourages entities to develop and submit additional examples of Implementation Guidance through a pre-qualified organization for endorsement consideration.

Some commenters requested that the SDT define "logical protection" or replace all instances of "logical protection" with "encryption."

The SDT contends that the standard is written to not specify a particular technology. This allows the requirement to be flexible in encompassing future protection solutions.

Some commenters recognized the SDT is not specifying the controls to be used to protect confidentiality and integrity and that the only examples provided in the implementation guidance include encryption. The commenters requested that the SDT provide other methods available to achieve the security objective if they exist. The commenter cited activities and specifications in FERC Order No. 822, such as key management between separate Responsible Entities that must be created and agreed upon by all registered entities involved in the data transfer. The commenter suggested such activities may not be achievable in the 24-month implementation period.

The commenter also noted that a Responsible Entity would lose Real-time Assessment and Real-time monitoring and control data if encryption failed. The commenter suggested a pilot to implement encryption.

The SDT agrees that there will be coordination necessary and designed R1.3 to have the involved entities document the responsibilities. The requirement has been written to allow flexibility on how entities work together on this requirement. The SDT notes there are a number of ways to demonstrate compliance with the requirement and encourages entities to develop and submit additional examples of Implementation Guidance through pre-qualified

organizations for endorsement consideration. Please see other comment responses on the 24 month implementation plan. The SDT has included the CIP Exceptional Circumstances language in the requirement in order to allow for encryption failures where reliability may require data to be transferred between Control Centers while the encryption capability is being repaired.

A commenter identified that on page 5 under section "Identification of Where Security Protection is applied by the Responsible Entity", language should be added to address the situation where a Responsible Entity does not manage either end of a communication link, indicating that this Responsible Entity does not have compliance obligations to R1.2.

The SDT agrees and has added such language to clarify obligations in such instances. Requirement 1.3 is also key in the documentation of such cases.

A couple of comments were received that the requirement should be less prescriptive, and additional technical and implementation guidance is needed to provide clarity on the SDT intent and audited scope.

The SDT asserts that the requirement is objective based and describes the risk to be mitigated without prescribing any technical solutions. There are a number of ways to demonstrate compliance with the requirement and the SDT encourages entities to develop and submit additional examples of Implementation Guidance through pre-qualified organizations for endorsement consideration.

Cost Effectiveness

A commenter expressed concern that if the data must be protected throughout the transmission, it would seem that could only be accomplished with encryption. The commenter noted that are cases where the existing equipment is not capable of encryption, replacement will be costly and implementation lengthy. In addition, the commenter stated that due to the large amount of applicable data, access to funds and budget cycle, and resources to perform work required, the solution will be costly.

The SDT has designed CIP-012 with flexibility so the entities can choose the most cost effective means to protect the data while being transmitted between Control Centers. The SDT agrees encryption will be a widely used method and can be accomplished at the application, network, transport, or physical layers or combinations thereof.

Some commenters noted that without clarity on ICCP between Control Centers, the commenters cannot be certain of what is expected, the costs or flexibility.

The SDT notes that data in scope may not be limited to ICCP. This is dependent on the specifics of each entity or entities.

A commenter acknowledged that more flexibility and less guidance could lead to inconsistency on requirement implementation among different entities.

CIP-012 is written to allow for selection of the most practical solution for the entity or entities.

A commenter questioned how the SDT is addressing the scenario where a Responsible Entity identifies multiple types of security protection and one of the forms fails but the data transmission is still protected, meeting the intent of the standard.

In the event of a failure of a protection method, it is the Entity's responsibility to demonstrate how compliance was maintained during the event.

A commenter does not agree the current standard and implementation plan can be executed in a cost effective manner. The commenter noted that encryption has been the only presented solution provided by auditors and SDT guidance to protect both confidentiality and integrity for the data within this scope. The commenter noted that more resources and capital will be required for a 24-month implementation versus a phased-in implementation. The commenter further noted that a phased implementation provides the ability to not only ensure the most effective plan, but also provides the ability to plan more accurately within budget cycles. In addition, the commenter noted that if encryption fails, an entity would lose Real-time Assessment and Real-time monitoring and control data. The commenter expressed concern that a 24-month implementation timeline would impact reliability as there are many opportunities for encryption to fail that must be addressed. The commenter suggested that this has a direct correlation on cost when addressing those opportunities during this timeframe. Additionally, the commenter requested the SDT draft reference models of methods that do not require encryption as a method to protect communications between Control Centers.

CIP-012 is written in a non-prescriptive manner to allow entities to select the protection methods that most appropriately fit their organization. This allows for logical or physical protection as appropriate. Regarding guidance, the SDT encourages entities to draft and submit guidance on other implementation examples.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2016-01 Modifications to CIP Standards

Draft Reliability Standard Audit Worksheet (RSAW) Posted for Industry Comment through July 2, 2018

Now Available

The draft RSAW for **CIP-012-1 – Cyber Security – Control Center Communication Networks** is posted on the project page for industry comment through **8 p.m. Eastern, Monday, July 2, 2018.** Submit feedback regarding the draft RSAW to RSAWfeedback@nerc.net.

For more information or assistance, contact Standards Developer, Jordan Mallory (via email) or at (404) 446-2589.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

CIP-012-1 is being posted for a 10-day final ballot.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23 - April 21, 2016
SAR posted for comment	June 1 – June 30, 2016
Informal comment period	February 10- March 13, 2017
45-day formal comment period with initial ballot	July 27 – September 11, 2017
45-day formal comment period with additional ballot	October 27 – December 11, 2017
45-day formal comment period with additional ballot	March 16 – April 30, 2018
45-day formal comment period with additional ballot	May 18 – July 2, 2018
10-day final ballot	August 3 – August 13, 2018
Anticipated Actions	**Date**
NERC Board	August 16, 2018

A. Introduction

1. **Title:** Cyber Security – Communications between Control Centers
2. **Number:** CIP-012-1

3. **Purpose:** To protect the confidentiality and integrity of Real-time Assessment and Real-time monitoring data transmitted between Control Centers.

4. **Applicability:**

   4.1. Functional Entities: The requirements in this standard apply to the following functional entities, referred to as "Responsible Entities," that own or operate a Control Center.

   4.1.1. Balancing Authority

   4.1.2. Generator Operator

   4.1.3. Generator Owner

   4.1.4. Reliability Coordinator

   4.1.5. Transmission Operator

   4.1.6. Transmission Owner

   4.2. Exemptions: The following are exempt from Reliability Standard CIP-012-1:

   4.2.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

   4.2.2. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

   4.2.3. A Control Center that transmits to another Control Center Real-time Assessment or Real-time monitoring data pertaining only to the generation resource or Transmission station or substation co-located with the transmitting Control Center.

5. **Effective Date:** See Implementation Plan for CIP-012-1.

B. Requirements and Measures

R1. The Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) to mitigate the risks posed by unauthorized disclosure and unauthorized modification of Real-time Assessment and Real-time monitoring data while being transmitted between any applicable Control Centers. The Responsible Entity is not required to include oral communications in its plan. The plan shall include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. Identification of security protection used to mitigate the risks posed by unauthorized disclosure and unauthorized modification of Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers;

1.2. Identification of where the Responsible Entity applied security protection for transmitting Real-time Assessment and Real-time monitoring data between Control Centers; and

1.3. If the Control Centers are owned or operated by different Responsible Entities, identification of the responsibilities of each Responsible Entity for applying security protection to the transmission of Real-time Assessment and Real-time monitoring data between those Control Centers.

M1. Evidence may include, but is not limited to, documented plan(s) that meet the security objective of Requirement R1 and documentation demonstrating the implementation of the plan(s).

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" (CEA) means NERC, the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- The Responsible Entities shall keep data or evidence of each Requirement in this Reliability Standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	N/A	The Responsible Entity documented its plan(s) but failed to include one of the applicable Parts of the plan as specified in Requirement R1.	The Responsible Entity documented its plan(s) but failed to include two of the applicable Parts of the plan as specified in Requirement R1.	The Responsible Entity failed to document plan(s) for Requirement R1; Or The Responsible Entity failed to implement any Part of its plan(s) for Requirement R1, except under CIP Exceptional Circumstances.

D. Regional Variances

None.

E. Associated Documents

Implementation Plan.

Technical Rationale for CIP-012-1.

Implementation Guidance.

Version History

Version	Date	Action	Change Tracking
1	TBD	Respond to FERC Order No. 822	N/A

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

~~This is the~~ CIP-012-1 is being posted for ~~fourth~~a 10-day ~~-~~final ballot~~draft of the proposed standard~~.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23 - April 21, 2016
SAR posted for comment	June 1 – June 30, 2016
Informal comment period	February 10- March 13, 2017
45-day formal comment period with initial ballot	July 27 – September 11, 2017
45-day formal comment period with additional ballot	October 27 – December 11, 2017
45-day formal comment period with additional ballot	March 16 – April 30, 2018
45-day formal comment period with additional ballot	May 18 – July 2, 2018
10-day final ballot	~~July 30~~August 3 – August ~~8~~13, 2018

Anticipated Actions	Date
~~10-day final ballot~~	~~July 30 – August 8, 2018~~
NERC Board	August 16, 2018

A. Introduction

1. **Title:** Cyber Security – Communications between Control Centers

2. **Number:** CIP-012-1

3. **Purpose:** To protect the confidentiality and integrity of Real-time Assessment and Real-time monitoring data transmitted between Control Centers.

4. **Applicability:**

   4.1. Functional Entities: The requirements in this standard apply to the following functional entities, referred to as "Responsible Entities," that own or operate a Control Center.

   4.1.1. Balancing Authority

   4.1.2. Generator Operator

   4.1.3. Generator Owner

   4.1.4. Reliability Coordinator

   4.1.5. Transmission Operator

   4.1.6. Transmission Owner

   4.2. Exemptions: The following are exempt from Reliability Standard CIP-012-1:

   4.2.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

   4.2.2. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

   4.2.3. A Control Center ~~at a generation resource or Transmission station or substation~~ that transmits to another Control Center Real-time Assessment or Real-time monitoring data pertaining only to the generation resource or Transmission station or substation co-located with ~~at which~~ the transmitting Control Center ~~is located~~.

5. **Effective Date:** See Implementation Plan for CIP-012-1.

B. Requirements and Measures

R1. The Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) to mitigate the risks ~~of~~ posed by unauthorized disclosure ~~or~~ and unauthorized modification of Real-time Assessment and Real-time monitoring data while being transmitted between any applicable Control Centers. The Responsible Entity is not required to include oral communications in its plan. The plan shall include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. Identification of security protection used to mitigate the risks posed by ~~of~~ unauthorized disclosure ~~or~~ and unauthorized modification of Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers;

1.2. Identification of where the Responsible Entity applied security protection for transmitting Real-time Assessment and Real-time monitoring data between Control Centers; and

1.3. If the Control Centers are owned or operated by different Responsible Entities, identification of~~y~~ the responsibilities of each Responsible Entity for applying security protection to the transmission of Real-time Assessment and Real-time monitoring data between those Control Centers.

M1. Evidence may include, but is not limited to, documented plan(s) that meet the security objective of Requirement R1 and documentation demonstrating the implementation of the plan(s).

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" (CEA) means NERC, the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- The Responsible Entities shall keep data or evidence of each Requirement in this Reliability Standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	N/A	The Responsible Entity documented its plan(s) but failed to include one of the applicable Parts of the plan as specified in Requirement R1.	The Responsible Entity documented its plan(s) but failed to include two of the applicable Parts of the plan as specified in Requirement R1.	The Responsible Entity failed to document plan(s) for Requirement R1; Or The Responsible Entity failed to implement any Part of its plan(s) for Requirement R1, except under CIP Exceptional Circumstances.

D. Regional Variances

None.

E. Associated Documents

Implementation Plan.

Technical Rationale for CIP-012-1.

Implementation Guidance.

Version History

Version	Date	Action	Change Tracking
1	TBD	Respond to FERC Order No. 822	N/A

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2016-02 Modifications to CIP Standards
Reliability Standard CIP-012-1

Applicable Standard

- Reliability Standard CIP-012-1 - Cyber Security – Communications between Control Centers

Requested Retirements

- None

Prerequisite Standard

These standard(s) or definitions must be approved before the Applicable Standard becomes effective:

- None

Applicable Entities

- Balancing Authority
- Generator Operator
- Generator Owner
- Reliability Coordinator
- Transmission Operator
- Transmission Owner

Effective Date

Reliability Standard CIP-012-1 - Cyber Security – Communications between Control Centers

Where approval by an applicable governmental authority is required, Reliability Standard CIP-012-1 shall become effective on the first day of the first calendar quarter that is twenty-four (24) calendar months after the effective date of the applicable governmental authority's order approving the standard, or as otherwise provided for by the applicable governmental authority.

Where approval by an applicable governmental authority is not required, Reliability Standard CIP-012-1 shall become effective on the first day of the first calendar quarter that is twenty-four (24) calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Violation Risk Factor and Violation Severity Level Justifications

Project 2016-02 Modifications to CIP Standards

This document provides the standard drafting team's (SDT's) justification for assignment of violation risk factors (VRFs) and violation severity levels (VSLs) for each requirement in **CIP-012-1**. Each requirement is assigned a VRF and a VSL. These elements support the determination of an initial value range for the Base Penalty Amount regarding violations of requirements in FERC-approved Reliability Standards, as defined in the Electric Reliability Organizations (ERO) Sanction Guidelines. The SDT applied the following NERC criteria and FERC Guidelines when developing the VRFs and VSLs for the requirements.

NERC Criteria for Violation Risk Factors

High Risk Requirement

A requirement that, if violated, could directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures, or could hinder restoration to a normal condition.

Medium Risk Requirement

A requirement that, if violated, could directly affect the electrical state or the capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System. However, violation of a medium risk requirement is unlikely to lead to Bulk Electric System instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System. However, violation of a medium risk requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to Bulk Electric System instability, separation, or cascading failures, nor to hinder restoration to a normal condition.

Lower Risk Requirement

A requirement that is administrative in nature and a requirement that, if violated, would not be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System; or, a requirement that is administrative in nature and a requirement in a planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.

FERC Guidelines for Violation Risk Factors

Guideline (1) – Consistency with the Conclusions of the Final Blackout Report

FERC seeks to ensure that VRFs assigned to Requirements of Reliability Standards in these identified areas appropriately reflect their historical critical impact on the reliability of the Bulk-Power System. In the VSL Order, FERC listed critical areas (from the Final Blackout Report) where violations could severely affect the reliability of the Bulk-Power System:

- Emergency operations
- Vegetation management
- Operator personnel training
- Protection systems and their coordination
- Operating tools and backup facilities
- Reactive power and voltage control
- System modeling and data exchange
- Communication protocol and facilities
- Requirements to determine equipment ratings
- Synchronized data recorders
- Clearer criteria for operationally critical facilities
- Appropriate use of transmission loading relief.

Guideline (2) – Consistency within a Reliability Standard

FERC expects a rational connection between the sub-Requirement VRF assignments and the main Requirement VRF assignment.

Guideline (3) – Consistency among Reliability Standards

FERC expects the assignment of VRFs corresponding to Requirements that address similar reliability goals in different Reliability Standards would be treated comparably.

Guideline (4) – Consistency with NERC's Definition of the Violation Risk Factor Level

Guideline (4) was developed to evaluate whether the assignment of a particular VRF level conforms to NERC's definition of that risk level.

Guideline (5) – Treatment of Requirements that Co-mingle More Than One Obligation

Where a single Requirement co-mingles a higher risk reliability objective and a lesser risk reliability objective, the VRF assignment for such Requirements must not be watered down to reflect the lower risk level associated with the less important objective of the Reliability Standard.

NERC Criteria for Violation Severity Levels

VSLs define the degree to which compliance with a requirement was not achieved. Each requirement must have at least one VSL. While it is preferable to have four VSLs for each requirement, some requirements do not have multiple "degrees" of noncompliant performance and may have only one, two, or three VSLs.

VSLs should be based on NERC's overarching criteria shown in the table below:

Lower VSL	Moderate VSL	High VSL	Severe VSL
The performance or product measured almost meets the full intent of the requirement.	The performance or product measured meets the majority of the intent of the requirement.	The performance or product measured does not meet the majority of the intent of the requirement, but does meet some of the intent.	The performance or product measured does not substantively meet the intent of the requirement.

FERC Order of Violation Severity Levels

The FERC VSL guidelines are presented below, followed by an analysis of whether the VSLs proposed for each requirement in the standard meet the FERC Guidelines for assessing VSLs:

Guideline (1) – Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance

Compare the VSLs to any prior levels of non-compliance and avoid significant changes that may encourage a lower level of compliance than was required when levels of non-compliance were used.

Guideline (2) – Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties

A violation of a "binary" type requirement must be a "Severe" VSL.

Do not use ambiguous terms such as "minor" and "significant" to describe noncompliant performance.

Guideline (3) – Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement

VSLs should not expand on what is required in the requirement.

Guideline (4) – Violation Severity Level Assignment Should Be Based on a Single Violation, Not on a Cumulative Number of Violations

Unless otherwise stated in the requirement, each instance of non-compliance with a requirement is a separate violation. Section 4 of the Sanction Guidelines states that assessing penalties on a per violation per day basis is the "default" for penalty calculations.

VRF Justifications for CIP-012-1, Requirement R1	
Proposed VRF	**Medium**
NERC VRF Discussion	A VRF of Medium was assigned to this requirement. Cyber security plans enable effective implementation of the CIP standard's requirements to mitigate the risks posed by unauthorized disclosure and unauthorized modification of data used for Real-time Assessments and Real-time monitoring while being transmitted between Control Centers.
FERC VRF G1 Discussion Guideline 1- Consistency with Blackout Report	N/A
FERC VRF G2 Discussion Guideline 2- Consistency within a Reliability Standard	N/A
FERC VRF G3 Discussion Guideline 3- Consistency among Reliability Standards	The requirement complements CIP-005-1, Requirement R1, CIP-006-6, Requirement R1, and CIP-007-6, Requirement R1 which are related to security of networks and communications components. The proposed VRF is consistent with these related requirements.
FERC VRF G4 Discussion Guideline 4- Consistency with NERC Definitions of VRFs	Failure to have the required plan would not, under Emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.
FERC VRF G5 Discussion	N/A

VRF Justifications for CIP-012-1, Requirement R1	
Proposed VRF	**Medium**
Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation	

VSLs for CIP-012-1, Requirement R1			
Lower	**Moderate**	**High**	**Severe**
N/A	The Responsible Entity documented its plan(s) but failed to include one of the applicable Parts of the plan as specified in Requirement R1.	The Responsible Entity documented its plan(s) but failed to include two of the applicable Parts of the plan as specified in Requirement R1.	The Responsible Entity failed to document plan(s) for Requirement R1; Or The Responsible Entity failed to implement any Part of its plan(s) for Requirement R1, except under CIP Exceptional Circumstances.

VSL Justifications for CIP-012-1 Requirements R1	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The requirement is new. Therefore, the proposed VSL does not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The requirement is for the Responsible Entity to implement one or more documented plan(s) as specified in Requirement R1. The moderate VSL addresses where the Responsible Entity documented its plan(s) but failed to include one of the applicable parts of the plan as specified in Requirement R1. The high VSL addresses where the Responsible Entity documented its plan(s) but failed to include two of the applicable parts of the plan as specified in Requirement R1. The severe VSL addresses where the Responsible Entity failed to document plan(s) for Requirement R1, or where the Responsible Entity failed to implement plan(s) for Requirement R1.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL uses the same terminology as used in the associated requirement and is, therefore, consistent with the requirement.

FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Each VSL is based on a single violation and not cumulative violations.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Violation Risk Factor and Violation Severity Level Justifications

Project 2016-02 Modifications to CIP Standards

This document provides the standard drafting team's (SDT's) justification for assignment of violation risk factors (VRFs) and violation severity levels (VSLs) for each requirement in **CIP-012-1**. Each requirement is assigned a VRF and a VSL. These elements support the determination of an initial value range for the Base Penalty Amount regarding violations of requirements in FERC-approved Reliability Standards, as defined in the Electric Reliability Organizations (ERO) Sanction Guidelines. The SDT applied the following NERC criteria and FERC Guidelines when developing the VRFs and VSLs for the requirements.

NERC Criteria for Violation Risk Factors

High Risk Requirement

A requirement that, if violated, could directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures, or could hinder restoration to a normal condition.

Medium Risk Requirement

A requirement that, if violated, could directly affect the electrical state or the capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System. However, violation of a medium risk requirement is unlikely to lead to Bulk Electric System instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System. However, violation of a medium risk requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to Bulk Electric System instability, separation, or cascading failures, nor to hinder restoration to a normal condition.

Lower Risk Requirement
A requirement that is administrative in nature and a requirement that, if violated, would not be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System; or, a requirement that is administrative in nature and a requirement in a planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.

FERC Guidelines for Violation Risk Factors

Guideline (1) – Consistency with the Conclusions of the Final Blackout Report

FERC seeks to ensure that VRFs assigned to Requirements of Reliability Standards in these identified areas appropriately reflect their historical critical impact on the reliability of the Bulk-Power System. In the VSL Order, FERC listed critical areas (from the Final Blackout Report) where violations could severely affect the reliability of the Bulk-Power System:

- Emergency operations
- Vegetation management
- Operator personnel training
- Protection systems and their coordination
- Operating tools and backup facilities
- Reactive power and voltage control
- System modeling and data exchange
- Communication protocol and facilities
- Requirements to determine equipment ratings
- Synchronized data recorders
- Clearer criteria for operationally critical facilities
- Appropriate use of transmission loading relief.

Guideline (2) – Consistency within a Reliability Standard

FERC expects a rational connection between the sub-Requirement VRF assignments and the main Requirement VRF assignment.

Guideline (3) – Consistency among Reliability Standards

FERC expects the assignment of VRFs corresponding to Requirements that address similar reliability goals in different Reliability Standards would be treated comparably.

Guideline (4) – Consistency with NERC's Definition of the Violation Risk Factor Level

Guideline (4) was developed to evaluate whether the assignment of a particular VRF level conforms to NERC's definition of that risk level.

Guideline (5) – Treatment of Requirements that Co-mingle More Than One Obligation

Where a single Requirement co-mingles a higher risk reliability objective and a lesser risk reliability objective, the VRF assignment for such Requirements must not be watered down to reflect the lower risk level associated with the less important objective of the Reliability Standard.

NERC Criteria for Violation Severity Levels

VSLs define the degree to which compliance with a requirement was not achieved. Each requirement must have at least one VSL. While it is preferable to have four VSLs for each requirement, some requirements do not have multiple "degrees" of noncompliant performance and may have only one, two, or three VSLs.

VSLs should be based on NERC's overarching criteria shown in the table below:

Lower VSL	Moderate VSL	High VSL	Severe VSL
The performance or product measured almost meets the full intent of the requirement.	The performance or product measured meets the majority of the intent of the requirement.	The performance or product measured does not meet the majority of the intent of the requirement, but does meet some of the intent.	The performance or product measured does not substantively meet the intent of the requirement.

FERC Order of Violation Severity Levels

The FERC VSL guidelines are presented below, followed by an analysis of whether the VSLs proposed for each requirement in the standard meet the FERC Guidelines for assessing VSLs:

Guideline (1) – Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance

Compare the VSLs to any prior levels of non-compliance and avoid significant changes that may encourage a lower level of compliance than was required when levels of non-compliance were used.

Guideline (2) – Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties

A violation of a "binary" type requirement must be a "Severe" VSL.

Do not use ambiguous terms such as "minor" and "significant" to describe noncompliant performance.

Guideline (3) – Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement

VSLs should not expand on what is required in the requirement.

Guideline (4) – Violation Severity Level Assignment Should Be Based on a Single Violation, Not on a Cumulative Number of Violations

Unless otherwise stated in the requirement, each instance of non-compliance with a requirement is a separate violation. Section 4 of the Sanction Guidelines states that assessing penalties on a per violation per day basis is the "default" for penalty calculations.

VRF Justifications for CIP-012-1, Requirement R1	
Proposed VRF	**Medium**
NERC VRF Discussion	A VRF of Medium was assigned to this requirement. Cyber security plans enable effective implementation of the CIP standard's requirements to mitigate the risks ~~of the~~posed by unauthorized disclosure ~~or~~ and unauthorized modification of data used for Real-time Assessments and Real-time monitoring while being transmitted between Control Centers.
FERC VRF G1 Discussion Guideline 1- Consistency with Blackout Report	N/A
FERC VRF G2 Discussion Guideline 2- Consistency within a Reliability Standard	N/A
FERC VRF G3 Discussion Guideline 3- Consistency among Reliability Standards	The requirement complements CIP-005-1, Requirement R1, CIP-006-6, Requirement R1, and CIP-007-6, Requirement R1 which are related to security of networks and communications components. The proposed VRF is consistent with these related requirements.
FERC VRF G4 Discussion Guideline 4- Consistency with NERC Definitions of VRFs	Failure to have the required~~a cyber security~~ plan would not, under Emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.
FERC VRF G5 Discussion	N/A

VRF Justifications for CIP-012-1, Requirement R1	
Proposed VRF	**Medium**
Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation	

VSLs for CIP-012-1, Requirement R1			
Lower	**Moderate**	**High**	**Severe**
N/A	The Responsible Entity documented its plan(s) but failed to include one of the applicable Parts of the plan as specified in Requirement R1.	The Responsible Entity documented its plan(s) but failed to include two of the applicable Parts of the plan as specified in Requirement R1.	The Responsible Entity failed to document plan(s) for Requirement R1; Or The Responsible Entity failed to implement any Part of its plan(s) for Requirement R1, except under CIP Exceptional Circumstances.

VSL Justifications for CIP-012-1 Requirements R1	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The requirement is new. Therefore, the proposed VSL does not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The requirement is for the Responsible Entity to implement one or more documented plan(s) as specified in Requirement R1. The moderate VSL addresses where the Responsible Entity documented its plan(s) but failed to include one of the applicable parts of the plan as specified in Requirement R1. The high VSL addresses where the Responsible Entity documented its plan(s) but failed to include two of the applicable parts of the plan as specified in Requirement R1. The severe VSL addresses where the Responsible Entity failed to document plan(s) for Requirement R1, or where the Responsible Entity failed to implement plan(s) for Requirement R1.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL uses the same terminology as used in the associated requirement and is, therefore, consistent with the requirement.

FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Each VSL is based on a single violation and not cumulative violations.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber Security – Communications between Control Centers

Technical Rationale and Justification for Reliability Standard CIP-012-1

August 2018

RELIABILITY | ACCOUNTABILITY



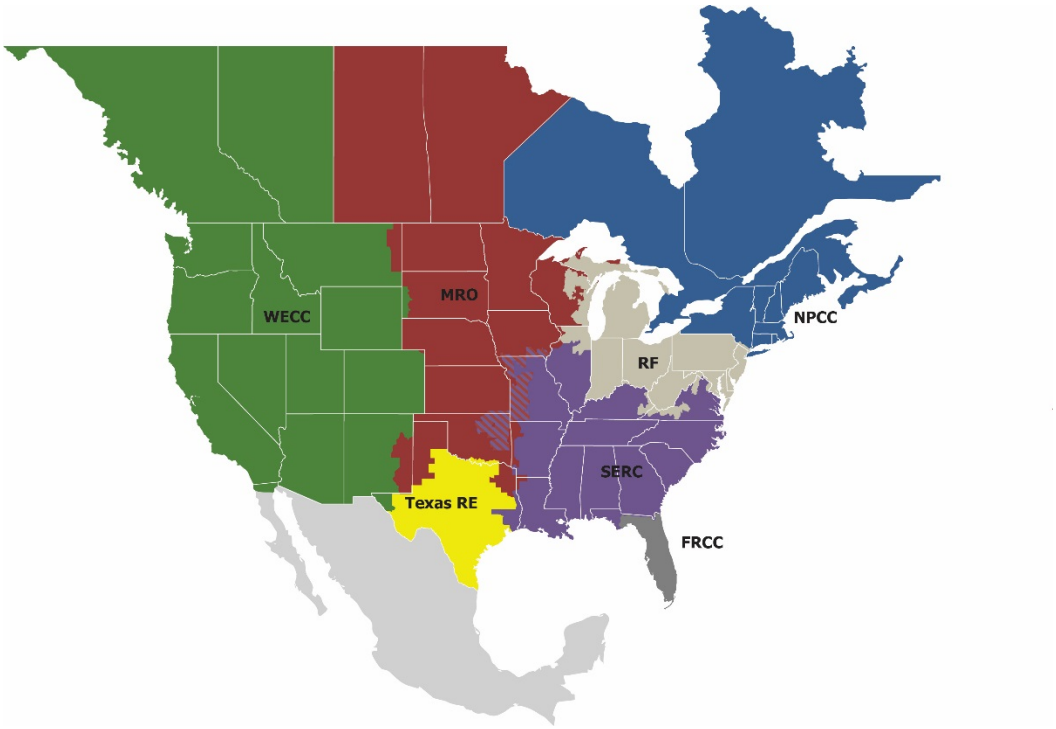

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Preface

The vision for the Electric Reliability Organization (ERO) Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the seven Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

The North American BPS is divided into seven RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.



FRCC	Florida Reliability Coordinating Council
MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-012-1. It will provide stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. It also contains information on the SDT's intent in drafting the requirements. This Technical Rationale and Justification for CIP-012-1 is not a Reliability Standard and should not be considered mandatory and enforceable.

On January 21, 2016, the Federal Energy Regulatory Commission (FERC or Commission) issued Order No. 822, approving seven Critical Infrastructure Protection (CIP) Reliability Standards and new or modified terms in the Glossary of Terms Used in NERC Reliability Standards, and directing modifications to the CIP Reliability Standards. Among others, the Commission directed the North American Electric Reliability Corporation (NERC) to "develop modifications to the CIP Reliability Standards to require Responsible Entities[1] to implement controls to protect, at a minimum, communication links and sensitive bulk electric system data communicated between bulk electric system Control Centers in a manner that is appropriately tailored to address the risks posed to the bulk electric system by the assets being protected (i.e., high, medium, or low impact)." (Order 822, Paragraph 53)

In response to the directive in Order No. 822, the Project 2016-02 standard drafting team (SDT) drafted Reliability Standard CIP-012-1 to require Responsible Entities to implement controls to protect sensitive Bulk Electric System (BES) data and communications links between BES Control Centers. Due to the sensitivity of the data being communicated between Control Centers, as defined in the Glossary of Terms Used in NERC Reliability Standards, the standard applies to all impact levels (i.e., high, medium, or low impact).

Although the Commission directed NERC to develop modifications to CIP-006, the SDT determined that modifications to CIP-006 would not be appropriate. There are differences between the plan(s) required to be developed and implemented for CIP-012-1 and the protection required in CIP-006-6 Requirement R1 Part 1.10. CIP-012-1 Requirements R1 and R2 protect the applicable data during transmission between two separate Control Centers. CIP-006-6 Requirement R1 Part 1.10 protects nonprogrammable communication components within an Electronic Security Perimeter (ESP) but outside of a Physical Security Perimeter (PSP). The transmission of applicable data between Control Centers takes place outside of an ESP. Therefore, the protection contained in CIP-006-6 Requirement R1 Part 1.10 does not apply.

The SDT drafted requirements to provide Responsible Entities the latitude to protect the communication links, the data, or both to satisfy the security objective consistent with the capabilities of the Responsible Entity's operational environment.

CIP-012 Exemption (4.2.3) for certain Control Centers

In the process of drafting CIP-012, the SDT became aware of certain generating plant or Transmission substation situations where such field assets could be dual-classified as Control Centers based on the current Control Center definition. Their communications to their BA or TOP Control Centers, however, are not included in the intended scope of CIP-012. This is because the communications do not differ from those of any other generating plant or substation. The SDT wrote an exemption (Section 4.2.3 within CIP-012) for this particular scenario which is described in further detail below.

I

[1] As used in the CIP Standards, a Responsible Entity refers to the registered entities subject to the CIP Standards.

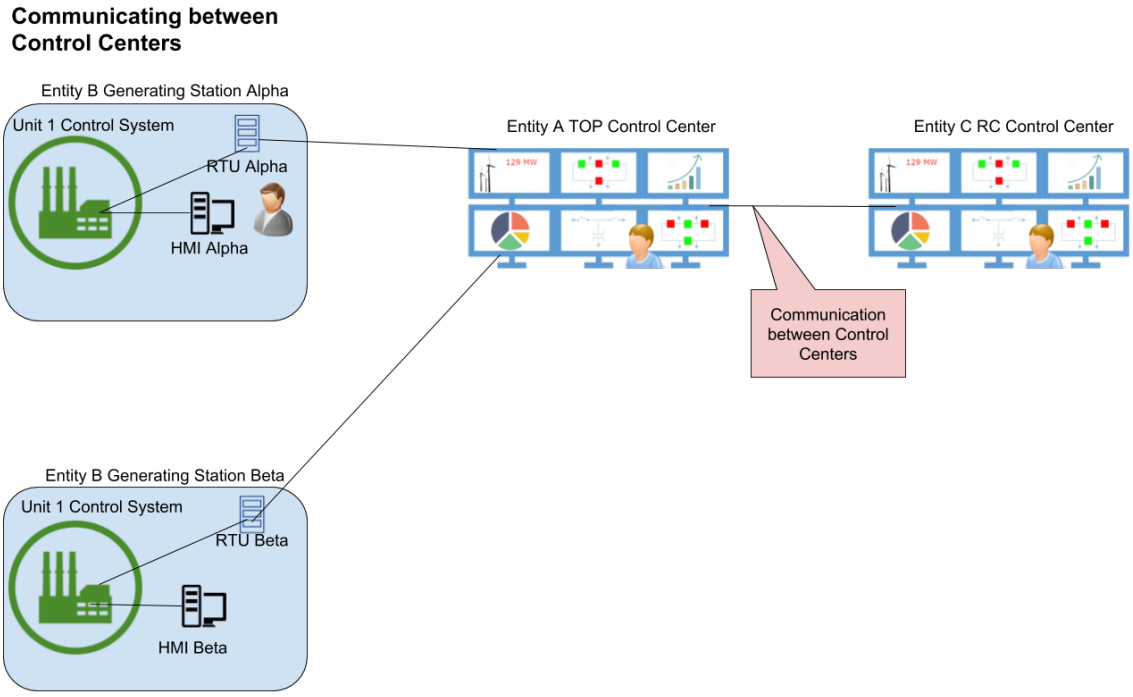


Figure 1

Figure 1 presents a typical scenario with two Control Centers communicating (in this instance Entity C's RC Control Center and Entity A's TOP Control Center). The communication between them is the intended scope of CIP-012's requirements if they meet the types of data inclusions and exclusions within the standard. The TOP Control Center is communicating with an RTU at two of Entity B's generating plants (Stations Alpha and Beta). Those RTU's are gathering information from each generating unit's control system. Each generating unit at each plant has an HMI (Human/Machine Interface; an operator workstation) that the local personnel use to operate their respective units.

Entity B decides that the generating unit at Station Beta, a small peaking facility, will only have an operator on site during the day. The operator at Station Alpha should be able to remotely start the unit at

Station Beta if necessary.

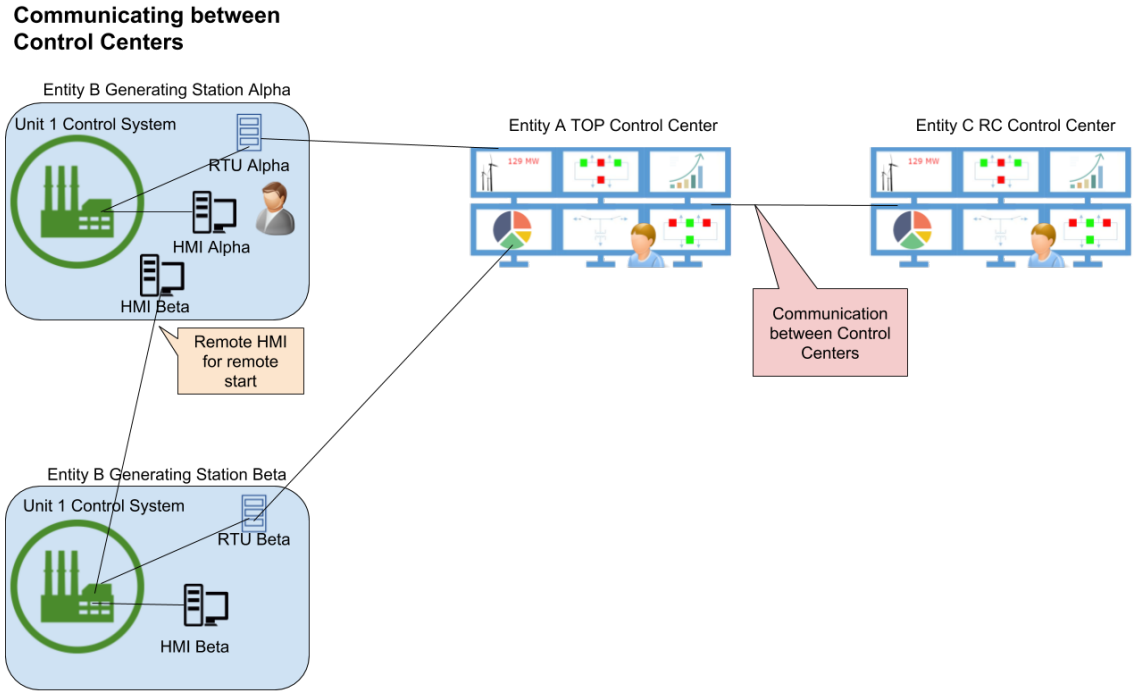


Figure 2

In Figure 2, Entity B installs a dedicated communications circuit from the control system on Station Beta's control system and puts a dedicated HMI at Station Alpha operator use. Station Alpha is now "one or more facilities hosting operating personnel that monitor and control the BES in real time to perform the reliability tasks of…a Generator Operator for generation Facilities at two or more locations" Because stations Alpha and Beta are two different plant locations. Station Alpha can now be dual-classified not only as a generation resource but also as a Control Center.

The communications to the TOP and RC Control Centers in Figure 1 have not changed. No new cyber systems are in place that can impact multiple units. In addition, no cyber systems have been added performing Control Center functions. The only change is that an HMI for Station Beta has been moved within close physical proximity to an HMI for Station Alpha.

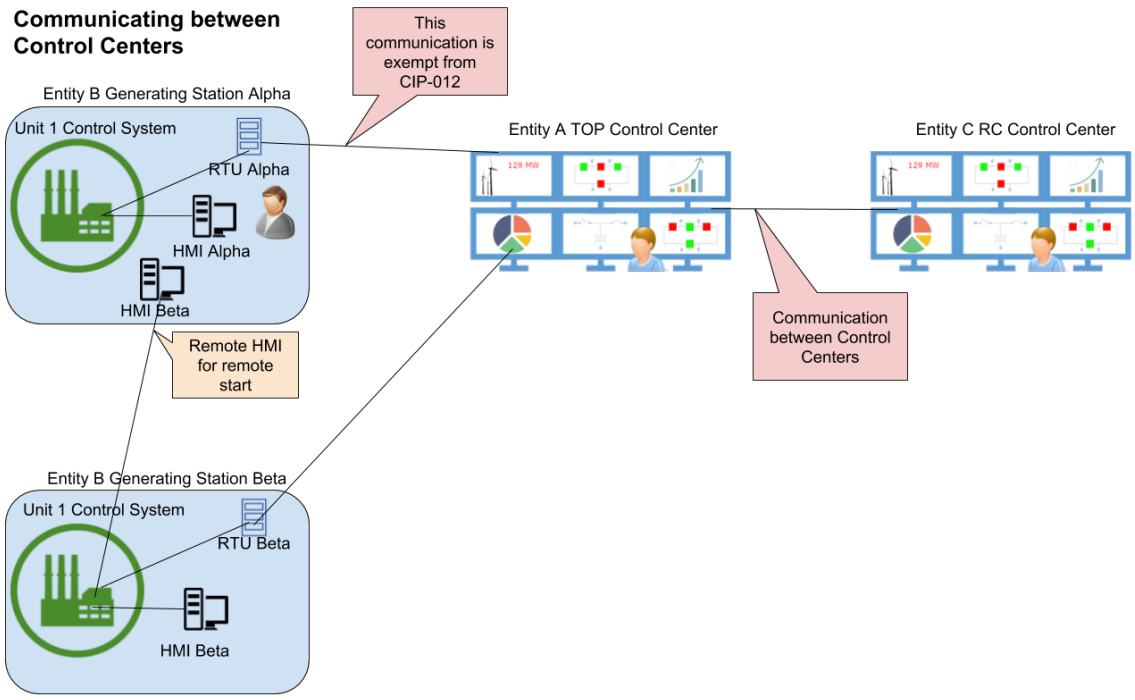


Figure 3

Although nothing has changed between them, this proximity makes the communication noted in Figure 3 between Station Alpha and Entity A's TOP Control Center subject to CIP-012 without the exemption. Two HMIs have been moved into the same room and a new NERC CIP standard applies to two entities.

This is an anomaly of the current Control Center definition of a facility, room, or building from which certain functions can be performed without regard to how they are done or what systems they are using. This is a generation specific example, but the potential situation exists where there are substations with an HMI or protective relay that "operating personnel" within the substation could use to impact an adjacent substation. It is also clear that in the criteria for TO's and GOP's the "two or more locations" is not a precise enough filter for defining what a Control Center truly is. The SDT's attempts to address this issue by clarifying the definition of Control Center pointed out larger issues that are not within the SDT's SAR to address at this time. Accordingly, the SDT is handling the issue through the 4.2.3 exemption within the CIP-012 standard which reads:

4.2.3. A Control Center g that transmits to another Control Center the transmitting Control Center.

The intent of this exemption is to exclude from CIP-012 the normal RTU-style communication from a field asset providing that field asset's status. Throughout this scenario or others like it, that communication has not changed and is still the same data pertaining only to the single location. The SDT recognizes that this communication is not the intent of the standard for protecting communications between Control Centers and this type of communications can be using older legacy communication technology and protocols.

The 4.2.3 exemption covers generation resources or Transmission station or substation locations that host operating personnel and can control BES Facilities at more than one location, possibly making them co-located Control Centers. The communication is exempt if each location is communicating the Real-time Assessment or Real-time monitoring data with another Control Center pertaining only to that location.

The above diagrams were generation specific. The following diagram is a more generic example:

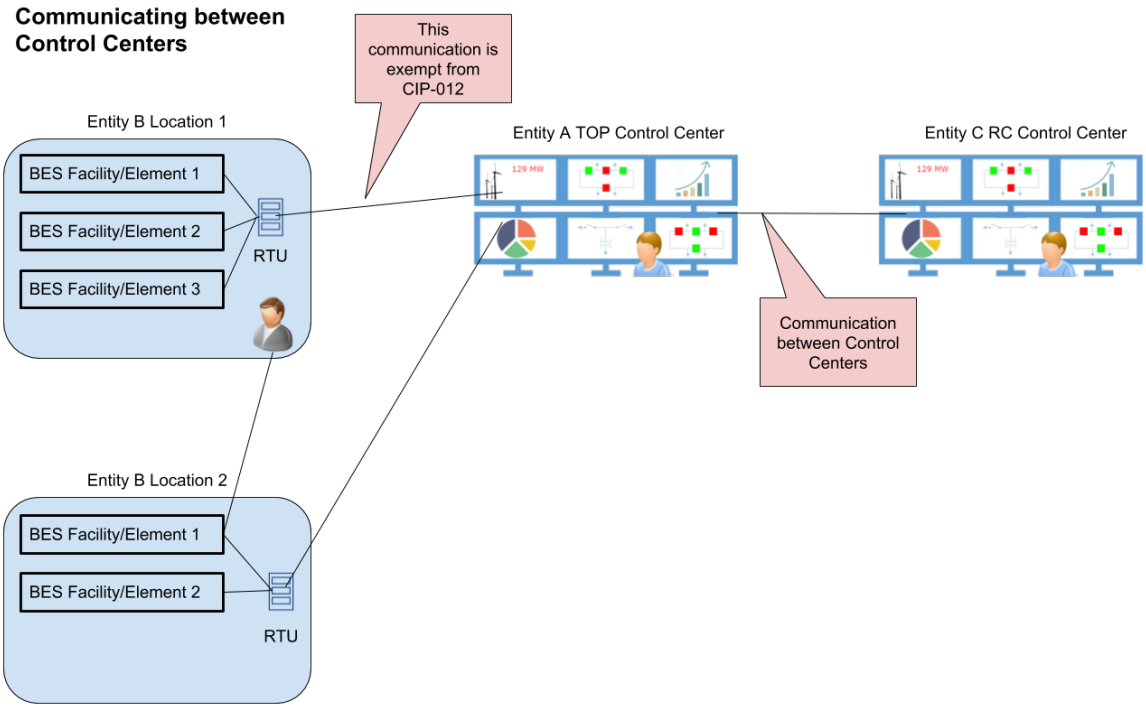


Figure 4

In Figure 4, each location is communicating only the Real-time Assessment or Real-time monitoring data pertaining to that single location. The communication from Entity B location one (1) to Entity A would be exempt from CIP-012-1.

If Location 2 communicates its data through Location 1,and Location 1 was both controlling and aggregating data from multiple locations to Entity A's TOP Control Center, the communication between Location 1 and Entity A's TOP Control Center would not be exempt from CIP-012.

Requirement R1

R1. The Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) to mitigate the risks posed by unauthorized disclosure and unauthorized modification of Real-time Assessment and Real-time monitoring data while being transmitted between any applicable Control Centers. The Responsible Entity is not required to include oral communications in its plan. The plan shall include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1 *Identification of security protection used to mitigate the risks posed by unauthorized disclosure and unauthorized modification of Real-time Assessment and Real-time monitoring while being transmitted between Control Centers;*

1.2 *Identification of where the Responsible Entity applied security protection for transmitting Real-time Assessment and Real-time monitoring data between Control Centers; and*

1.3 *If the Control Centers are owned or operated by different Responsible Entities, identification of the responsibilities of each Responsible Entity for applying security protection to the transmission of Real-time Assessment and Real-time monitoring data between those Control Centers.*

General Considerations for Requirement R1

Requirement R1 focuses on implementing a documented plan to protect information that is critical to the Real-time operations of the Bulk Electric System while in transit between applicable Control Centers. The SDT does not intend for the listed order of the three requirement parts to convey any sequence or significance.

Overview of confidentiality and integrity

The SDT drafted CIP-012-1 to address confidentiality and integrity of Real-time Assessment and Real-time monitoring data. This is accomplished by drafting the requirement to mitigate the risks posed by unauthorized disclosure (confidentiality) and unauthorized modification (integrity). For this Standard, the SDT relied on the definitions of confidentiality and integrity as defined by National Institute of Standards and Technology (NIST):

- Confidentiality is defined as, "Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information."[2]
- Integrity is defined as, "Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity."[3]

The SDT asserts that the availability of this data is already required by the performance obligation of the Operating and Planning Reliability Standards. The SDT drafted CIP-012-1 to address the data while being transmitted. The SDT maintains that this data resides within BES Cyber Systems, and while at rest is protected by CIP-003-6 through CIP-011-2.

Alignment with IRO and TOP standards

The SDT recognized the FERC reference to additional Reliability Standards and the responsibilities to protect the applicable data in accordance with NERC Reliability Standards TOP-003 and IRO-010. The SDT used these references to drive the identification of sensitive BES data and chose to base the CIP-012-1 requirements on the Real-time data

[2] NIST Special Publication 800-53A, Revision 4, page B-3
[3] NIST Special Publication 800-53A, Revision 4, page B-6

specification elements in these standards. This approach provides consistent scoping of identified data, and does not require each entity to devise its own list or inventory of this data. Many entities are required to provide this data under agreements executed with their RC, BA or TOP. Data requiring protection in CIP-012-1 consists of a subset of data that is identified by the RC, BA, and TOP in the TOP-003 and IRO-010 data specification standards, limited to Real-time Assessment data and Real-time monitoring data. CIP-012-1 excludes other data typically transferred between Control Centers such as Operational Planning Analysis data, weather data, market data, and other data that is not used by the RC, BA, and TOP to perform Real-time reliability assessments and analysis identified in TOP-003 and IRO-010. The SDT determined that Operational Planning Analysis data, if rendered unavailable, degraded, or misused, would not adversely impact the reliable operation of the BES within 15 minutes of the activation or exercise of the compromise as detailed in CIP-002- 5.1a. The SDT notes that there may be special instances during which Real-time Assessment or Real-time monitoring data is not identified by the RC, BA, or TOP. This would include data that may be exchanged between a Responsible Entity's primary and backup Control Center.

Identification of Where Security Protection is Applied by the Responsible Entity

The SDT noted the need for a Responsible Entity to identify where it will apply protection for applicable data. The SDT did not specify the location where CIP-012-1 security protection must be applied. This allows latitude for Responsible Entities to implement the security controls in a manner best fitting their individual circumstances. This latitude ensures entities can still take advantage of security measures, such as deep packet inspection implemented at or near the EAP when ESPs are present, while maintaining the capability to protect the applicable data being transmitted between Control Centers.

The SDT also recognizes that CIP-012 security protection may be applied to a Cyber Asset that is not an identified BES Cyber Asset, Protected Cyber Asset, or EACMS. The identification of the Cyber Asset as the location where security protection is applied does not expand the scope of Cyber Assets identified as applicable under Cyber Security Standards CIP-002 through CIP-011.

The SDT understands that in data exchanges between Control Centers, a single entity may not be responsible for both ends of the communication link. The SDT intends for a Responsible Entity to identify only where it applied security protection. The Responsible Entity should not be held accountable for identifying where a neighboring entity applied security protection at the neighboring entity's facility. A Responsible Entity, however, may decide to take responsibility for both ends of a communication link. For example, it may place a router in a neighboring entity's data center. In a scenario where a Responsible Entity has taken responsibility for applying security protection on both ends of the communication link, the Responsible Entity should identify where it applied security protection at both ends of the link. The SDT intends for there to be alignment between the identification of where security protection is applied in CIP-012-1 Requirement R1, Part 1.2 and the identification of Responsible Entity responsibilities in CIP-012-1 Requirement R1, Part 1.3.

Control Center Ownership

The standard requirements address protection for Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers owned by a single Responsible Entity. They also cover the applicable data transmitted between Control Centers owned by two or more separate Responsible Entities. Unlike protection between a single Responsible Entity's Control Centers, applying protection between Control Centers owned by more than one Responsible Entity requires additional coordination. The requirements do not explicitly require formal agreements between Responsible Entities partnering for protection of applicable data. It is strongly recommended, however, that these partnering entities develop agreements, or use existing ones, to define responsibilities to ensure the security objective is met. An example noted in FERC Order No. 822 Paragraph 59 is, "if several registered entities have joint responsibility for a cryptographic key management system used between their respective Control Centers, they should have the prerogative to come to a consensus on which organization administers that particular key management system."

As an example, Figure 5 shows several data transmissions between Control Centers that a Responsible Entity should consider to be in-scope. The example does not include all possible scenarios. The solid green lines are in-scope communications and the dashed red lines are out-of-scope communications.

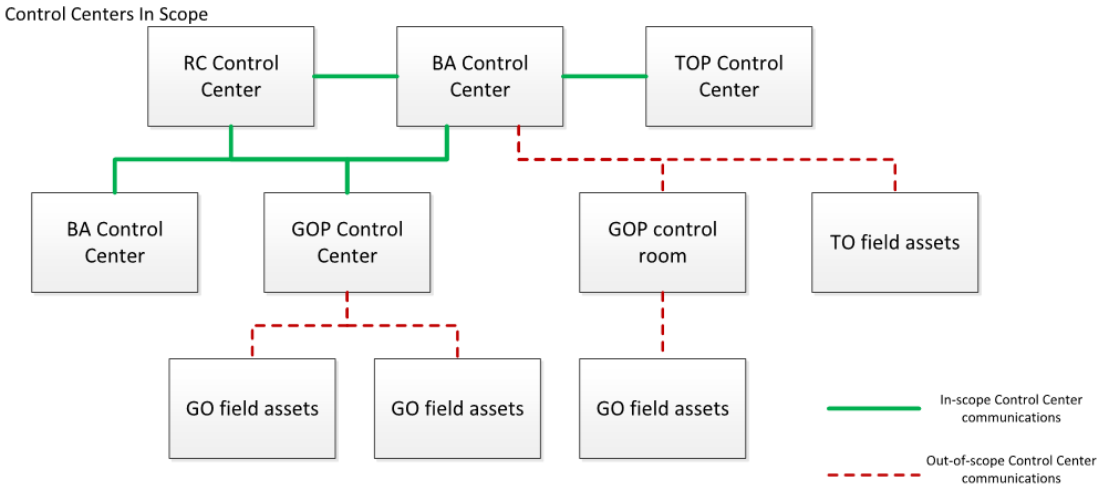


Figure 5: This reference model is an example and does not include all possible scenarios.

The SDT included Part 1.3 of the plan to address the situation when multiple registered entities are involved with protecting the data transmitted between Control Centers. Part 1.3 provides a mechanism to specify which entity is responsible for the application of security controls. The SDT included this requirement part to address security concerns as well as audit concerns. Where data is transmitted between different entities, the SDT asserts that it is necessary for both entities to understand the responsibilities of applying security controls to ensure the data is protected through its entire transmission and there is no security gap. The SDT also asserts this requirement part will provide evidence which may prevent the simultaneous auditing of multiple entities for each communication link between Control Centers when operated by different Responsible Entities. Security controls applied by the entity to achieve compliance with Parts 1.1 and 1.2 of the plan should correlate to the documented responsibilities in Part 1.3 of the entity's plan.

References

Here are several references to assist entities in developing plan(s) for protection of communication links:

- NIST Special Publication 800-53A, Revision 4: Security and Privacy Controls for Federal Information Systems and Organizations
- NIST Special Publication 800-82: Guide to Industrial Control Systems (ICS) Security
- NIST Special Publication 800-175B: Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms
- NIST Special Publication 800-47: Security Guide for Interconnecting Information Technology Systems

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

~~DRAFT~~

Cyber Security – Communications between Control Centers

Technical Rationale and Justification for Reliability Standard CIP-012-1

~~July~~ August 2018

RELIABILITY | ACCOUNTABILITY



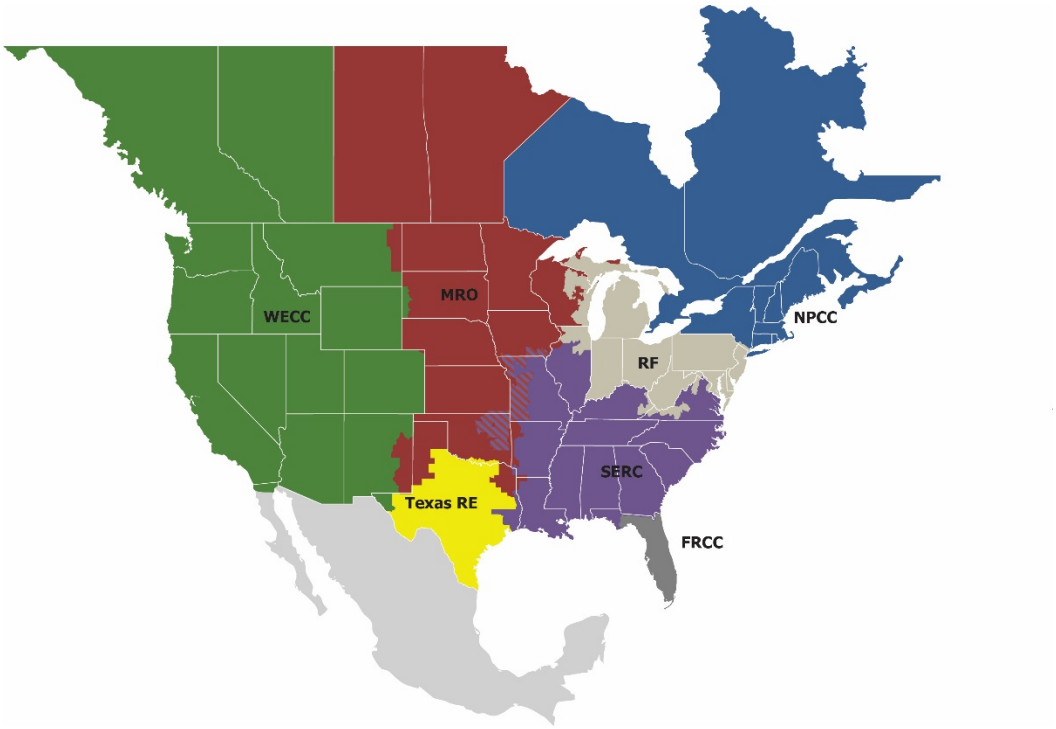

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Preface

The vision for the Electric Reliability Organization (ERO) Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the seven Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

The North American BPS is divided into seven RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.



FRCC	Florida Reliability Coordinating Council
MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-012-1. It will provide stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. It also contains information on the SDT's intent in drafting the requirements. This Technical Rationale and Justification for CIP-012-1 is not a Reliability Standard and should not be considered mandatory and enforceable.

On January 21, 2016, the Federal Energy Regulatory Commission (FERC or Commission) issued Order No. 822, approving seven Critical Infrastructure Protection (CIP) Reliability Standards and new or modified terms in the Glossary of Terms Used in NERC Reliability Standards, and directing modifications to the CIP Reliability Standards. Among others, the Commission directed the North American Electric Reliability Corporation (NERC) to "develop modifications to the CIP Reliability Standards to require Responsible Entities[1] to implement controls to protect, at a minimum, communication links and sensitive bulk electric system data communicated between bulk electric system Control Centers in a manner that is appropriately tailored to address the risks posed to the bulk electric system by the assets being protected (i.e., high, medium, or low impact)." (Order 822, Paragraph 53)

In response to the directive in Order No. 822, the Project 2016-02 standard drafting team (SDT) drafted Reliability Standard CIP-012-1 to require Responsible Entities to implement controls to protect sensitive Bulk Electric System (BES) data and communications links between BES Control Centers. Due to the sensitivity of the data being communicated between Control Centers, as defined in the Glossary of Terms Used in NERC Reliability Standards, the standard applies to all impact levels (i.e., high, medium, or low impact).

Although the Commission directed NERC to develop modifications to CIP-006, the SDT determined that modifications to CIP-006 would not be appropriate. There are differences between the plan(s) required to be developed and implemented for CIP-012-1 and the protection required in CIP-006-6 Requirement R1 Part 1.10. CIP-012-1 Requirements R1 and R2 protect the applicable data during transmission between two separate Control Centers. CIP-006-6 Requirement R1 Part 1.10 protects nonprogrammable communication components within an Electronic Security Perimeter (ESP) but outside of a Physical Security Perimeter (PSP). –The transmission of applicable data between Control Centers takes place outside of an ESP. Therefore, the protection contained in CIP-006-6 Requirement R1 Part 1.10 does not apply.

The SDT drafted requirements to provide Responsible Entities the latitude to protect the communication links, the data, or both to satisfy the security objective consistent with the capabilities of the Responsible Entity's operational environment.

CIP-012 Exemption (4.2.3) for certain Control Centers

~~As the SDT~~In the process of drafting~~ed~~ CIP-012, ~~i~~the SDT became aware of certain generating plant or Transmission substation situations where such field assets could be dual-classified as Control Centers based on the current Control Center definition. ~~However, t~~Their communications to their ~~normal~~ BA or TOP Control Centers, however, are not included in ~~are not the type of communications that are~~ the intended scope of CIP-012. This is because the communications ~~as they~~ do not differ from those of any other generating plant or substation. The SDT wrote an exemption (Section 4.2.3 within CIP-012) for this particular scenario which is described in further detail below.
I

[1] As used in the CIP Standards, a Responsible Entity refers to the registered entities subject to the CIP Standards.

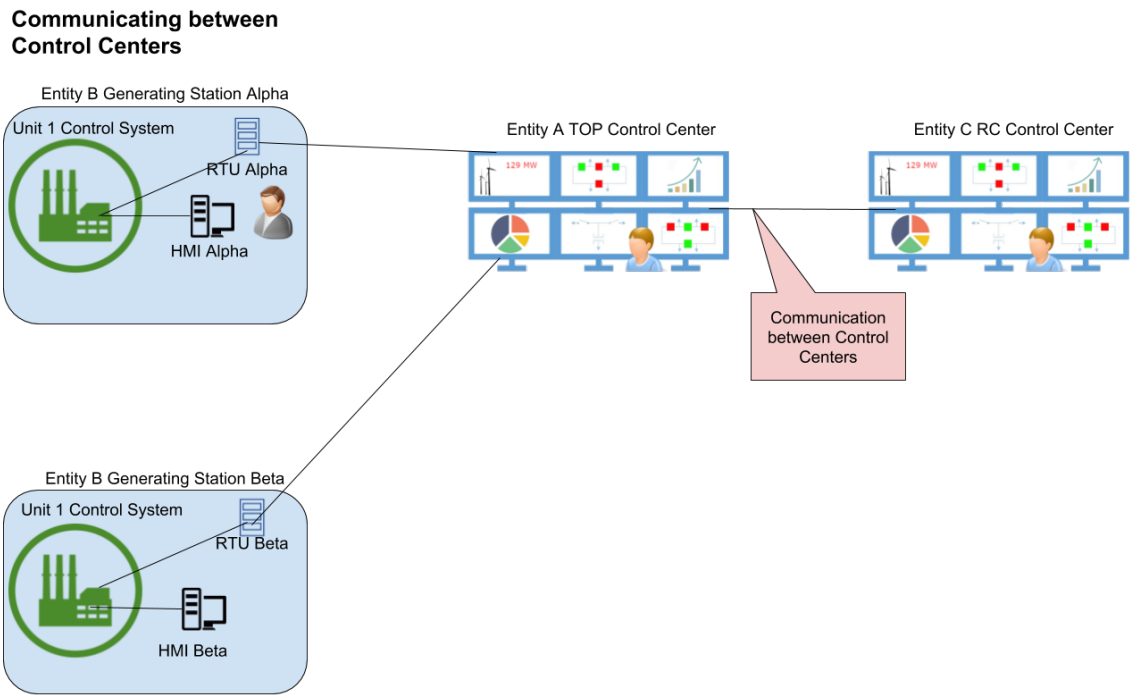


Figure 1

Figure 1 ~~above pictures~~ presents a typical scenario with two Control Centers communicating (in this instance Entity C's RC Control Center and Entity A's TOP Control Center). The communication between them is the intended scope of CIP-012's requirements if ~~it~~ they meet~~s~~ the types of data inclusions and exclusions within the standard. The TOP Control Center is communicating with an RTU at two of Entity B's generating plants (Stations Alpha and Beta). ~~and t~~Those RTU's are gathering information from each generating unit's control system. Each generating unit at each plant has an HMI (Human/Machine Interface; an operator workstation) that the local personnel use to operate their respective units.

Entity B decides that the generating unit at Station Beta, a small peaking facility, will only have an operator on site during the day. ~~and t~~The operator at Station Alpha should be able to remotely start the

unit at Station Beta if necessary.

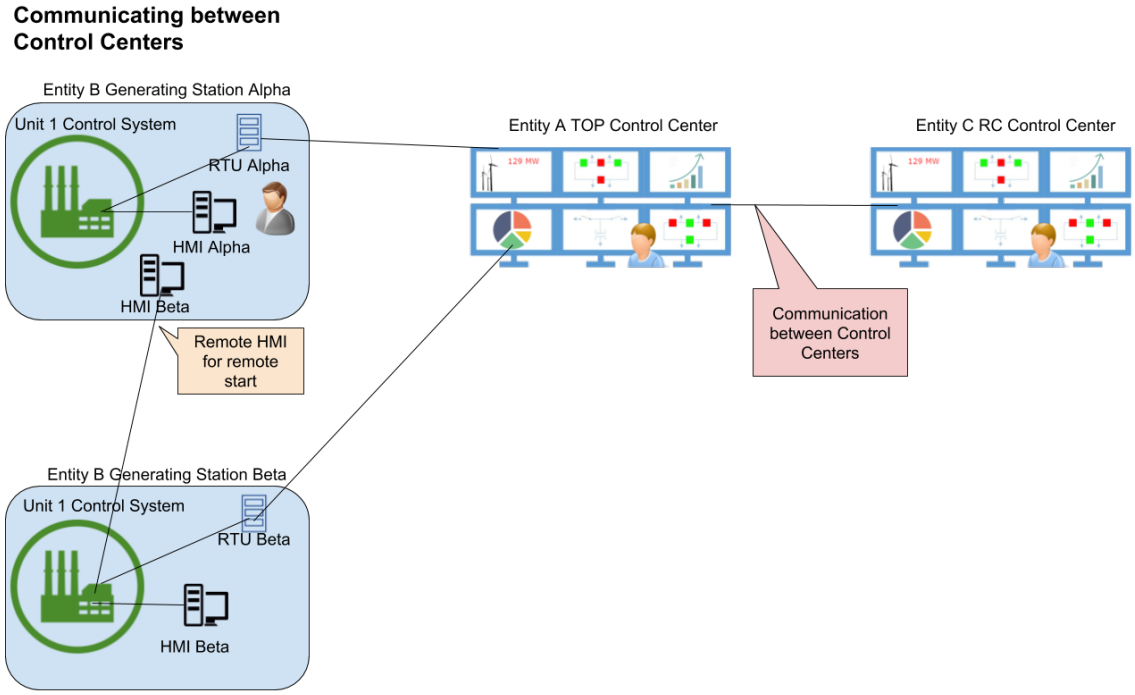


Figure 2

In Figure 2, Entity B installs a dedicated communications circuit from the control system on Station Beta's control system and puts a dedicated HMI at Station Alpha ~~the~~ operator ~~can~~ use. Station Alpha is now "one or more facilities hosting operating personnel that monitor and control the BES in real time to perform the reliability tasks of…a Generator Operator for generation Facilities at two or more locations~~.~~" Because stations Alpha and Beta are two different plant locations. Station Alpha ~~It~~ can now be dual-classified not only as a generation resource but also as a Control Center.

The communications to the TOP and RC Control Centers ~~from~~ in Figure 1 have not changed ~~at all~~. No new cyber systems are in place that can impact multiple units. In addition, ~~N~~no cyber systems have been added performing Control Center functions. ~~No additional risk from cyber systems has been added.~~ The only ~~thing that has~~ change~~d~~ is that an HMI for Station Beta has been moved within close physical proximity to an HMI for Station Alpha.

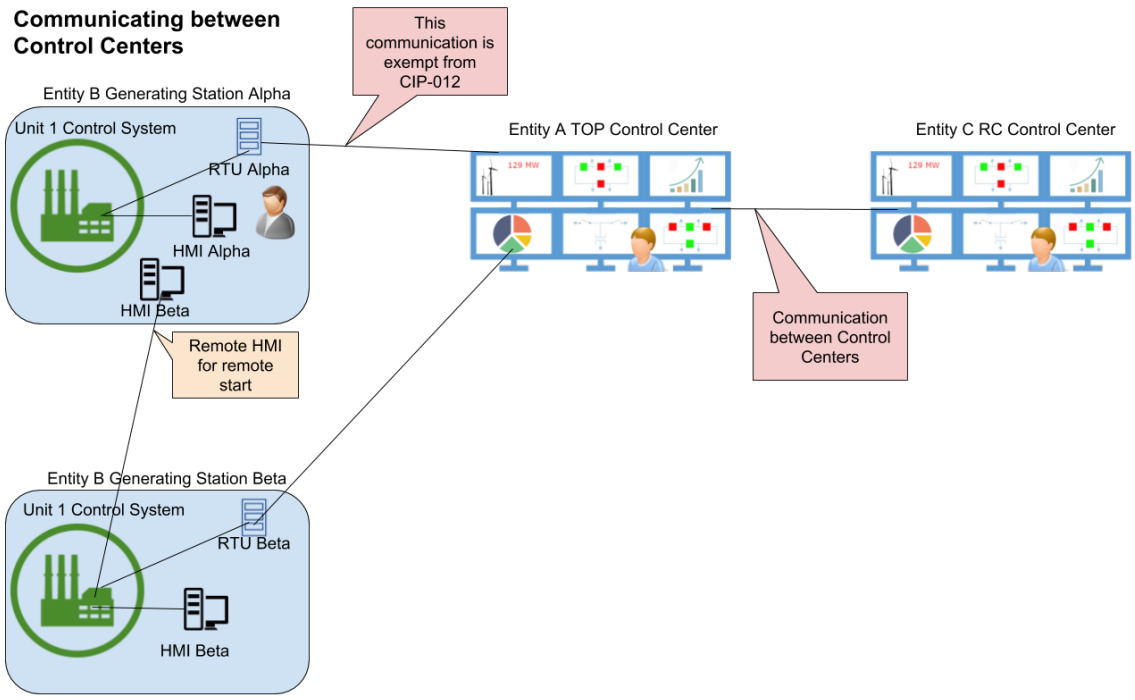


Figure 3

~~The SDT realized how this suddenly makes~~ Although nothing has changed between them, this proximity makes the communication noted in Figure 3 between Station Alpha and Entity A's TOP Control Center subject to CIP-012 ~~although nothing has changed between them~~without the exemption. ~~There is no new risk involved.~~ Two HMI~~'~~s have been moved into the same room and ~~suddenly~~ a new NERC CIP standard applies to two entities.

This is an ~~anamoly~~ anomaly of the current Control Center definition ~~defining~~ of a facility, room, or building from which ~~something~~ certain functions can be ~~done~~ performed without regard to how ~~its~~ they are done or ~~with~~ what systems they are using. This is a generation specific example, but the ~~SDT can envision~~potential situation exists where there are substations with an HMI or protective relay that "operating personnel" within the substation could use to impact an adjacent substation. ~~The SDT realizes~~It is also clear that in the criteria for TO's and GOP's the "two or more ~~geographic~~ locations" is not a precise enough filter for ~~capturing~~ defining what a Control Center truly is. The SDT's attempts to address this issue by clarifying the definition of Control Center pointed out larger issues that are not within the SDT's SAR to address at this time. ~~Therefore~~ Accordingly, the SDT is handling the issue ~~this creates for CIP-012 by~~through the 4.2.3 exemption within the CIP-012 standard which reads:

> 4.2.3. A Control Center g~~eneration resource or Transmission station or substation~~ that transmits to another Control Center ~~at which~~ the transmitting Control Center. ~~is located~~

The intent of this exemption is to exclude from CIP-012 the normal RTU-style communication from a field asset ~~about~~ providing that field asset's status ~~from CIP-012~~. Throughout this scenario or others like it, that communication has not changed and is still the same data pertaining only to the single location. The SDT recognizes that this communication is not the intent of the standard for protecting communications between Control Centers and this type of communications can be using older legacy communication technology and protocols.

The 4.2.3 exemption covers generation resources or Transmission station or substation locations that host operating personnel and can control BES Facilities at more than one location, possibly making them co-located

Control Centers. The communication is exempt if each location is communicating the Real-time Assessment or Real-time monitoring data with another Control Center pertaining only to that location.

The above diagrams were generation specific. The following diagram is a more generic example:

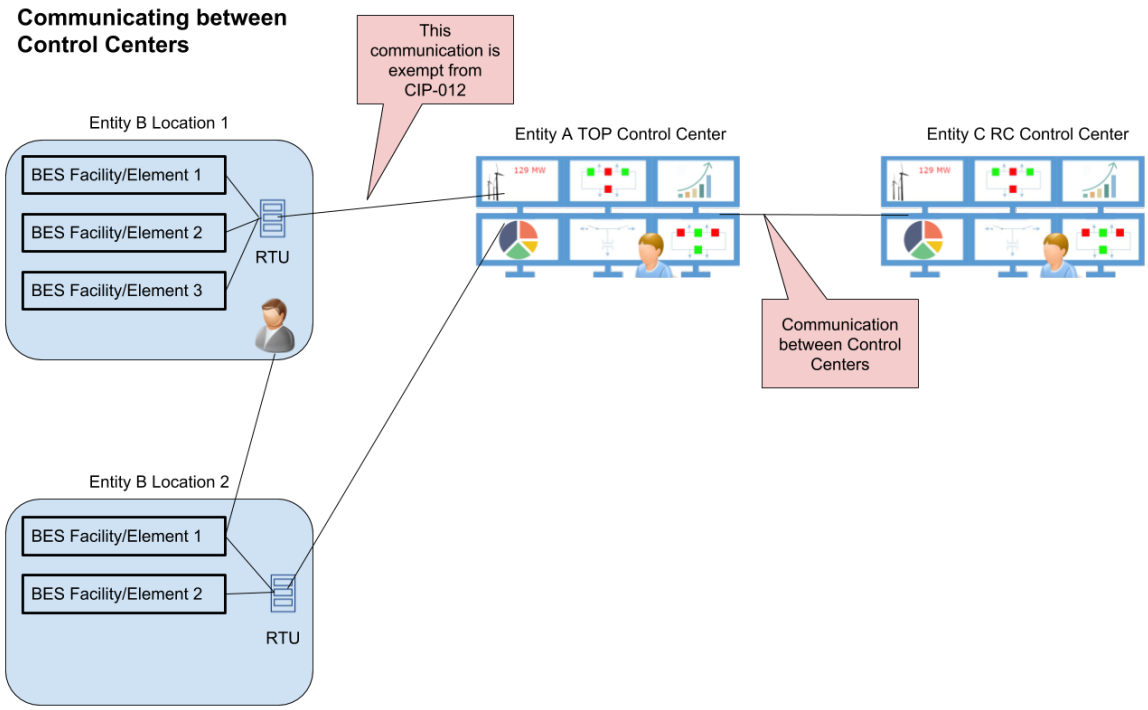


Figure 4

In Figure 4, each location is communicating only the Real-time Assessment or Real-time monitoring data pertaining to that single location. -The communication from Entity B location one (1) to Entity A would be exempt from CIP-012-1.

If Location 2 communicateds its data through Location 1,and Location 1 was both controlling and aggregating data from multiple locations to Entity A's TOP Control Center, the communication between Location 1 and Entity A's TOP Control Center would not be exempt from CIP-012.

Requirement R1

R1. The Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) to mitigate the risks ~~of~~posed by unauthorized disclosure and~~or~~ unauthorized modification of Real-time Assessment and Real-time monitoring data while being transmitted between any applicable Control Centers. The Responsible Entity is not required to include oral communications in its plan. The plan shall include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1 *Identification of security protection used to mitigate the risks ~~of~~ posed by unauthorized disclosure and~~or~~ unauthorized modification of Real-time Assessment and Real-time monitoring while being transmitted between Control Centers;*

1.2 *Identification of where the Responsible Entity applied security protection for transmitting Real-time Assessment and Real-time monitoring data between Control Centers; and*

1.3 *If the Control Centers are owned or operated by different Responsible Entities, identification of~~y~~ the responsibilities of each Responsible Entity for applying security protection to the transmission of Real-time Assessment and Real-time monitoring data between those Control Centers.*

General Considerations for Requirement R1

Requirement R1 focuses on implementing a documented plan to protect information that is critical to the Real-time operations of the Bulk Electric System while in transit between applicable Control Centers. The SDT does not intend for the listed order of the three requirement parts to convey any sequence or significance.

Overview of confidentiality and integrity

The SDT drafted CIP-012-1 to address confidentiality and integrity of Real-time Assessment and Real-time monitoring data. This is accomplished by drafting the requirement to mitigate the risks ~~of~~ posed by unauthorized disclosure (confidentiality) ~~or~~ and unauthorized modification (integrity). For this Standard, the SDT relied on the definitions of confidentiality and integrity as defined by National Institute of Standards and Technology (NIST):

- Confidentiality is defined as, "Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information."[2]
- Integrity is defined as, "Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity."[3]

The SDT asserts that the availability of this data is already required by the performance obligation of the Operating and Planning Reliability Standards. The SDT drafted CIP-012-1 to address the data while being transmitted. The SDT maintains that this data resides within BES Cyber Systems, and while at rest is protected by CIP-003-6 through CIP-011-2.

Alignment with IRO and TOP standards

The SDT recognized the FERC reference to additional Reliability Standards and the responsibilities to protect the applicable data in accordance with NERC Reliability Standards TOP-003 and IRO-010. The SDT used these references to drive the identification of sensitive BES data and chose to base the CIP-012-1 requirements on the Real-time data

[2] NIST Special Publication 800-53A, Revision 4, page B-3
[3] NIST Special Publication 800-53A, Revision 4, page B-6

specification elements in these standards. ~~-~~This approach provides consistent scoping of identified data, and does not require each entity to devise its own list or inventory of this data. Many entities are required to provide this data under agreements executed with their RC, BA or TOP. ~~-~~Data requiring protection in CIP-012-1 consists of a subset of data that is identified by the RC, BA, and TOP in the TOP-003 and IRO-010 data specification standards, limited to Real-time Assessment data and Real-time monitoring data. CIP-012-1 excludes other data typically transferred between Control Centers such as Operational Planning Analysis data, weather data, market data, and other data that is not used by the RC, BA, and TOP to perform Real-time reliability assessments and analysis identified in TOP-003 and IRO-010. The SDT determined that Operational Planning Analysis data, if rendered unavailable, degraded, or misused, would not adversely impact the reliable operation of the BES within 15 minutes of the activation or exercise of the compromise as detailed in CIP-002- 5.1a. ~~However, t~~The SDT note~~d~~ that there may be special instances during which Real-time Assessment or Real-time ~~Monitoring~~ monitoring data is not identified by the RC, BA, or TOP. This would include data that may be exchanged between a Responsible Entity's primary and backup Control Center.

Identification of Where Security Protection is Applied by the Responsible Entity

The SDT noted the need for a Responsible Entity to identify where it will apply protection for applicable data. The SDT did not specify the location where CIP-012-1 security protection must be applied. This allows ~~to provide~~ latitude for Responsible Entities to implement the security controls in a manner best fitting their individual circumstances. ~~-~~This latitude ensures entities can still take advantage of security measures, such as deep packet inspection implemented at or near the EAP when ESPs are present, while maintaining the capability to protect the applicable data being transmitted between Control Centers.

The SDT also recognizes that CIP-012 security protection may be applied to a Cyber Asset that is not an identified BES Cyber Asset, Protected Cyber Asset, or EACMS. ~~-~~The identification of the Cyber Asset as the location where security protection is applied does not expand the scope of Cyber Assets identified as applicable under Cyber Security Standards CIP-002 through CIP-011.

The SDT understands that in data exchanges between Control Centers, a single entity may not be responsible for both ends of the communication link. ~~-~~The SDT intends for a Responsible Entity to identify only where it applied security protection. ~~-~~The Responsible Entity should not be held accountable for identifying where a neighboring entity applied security protection at the neighboring entity's facility. ~~-~~A Responsible Entity, however, may decide to take responsibility for both ends of a communication link. For example, it may place a router in a neighboring entity's data center. ~~-~~In a scenario ~~like this,~~ where a Responsible Entity has taken responsibility for applying security protection on both ends of the communication link, the Responsible Entity should identify where it applied security protection at both ends of the link. ~~-~~The SDT intends for there to be alignment between the identification of where security protection is applied in CIP-012-1 Requirement R1, Part 1.2 and the identification of Responsible Entity responsibilities in CIP-012-1 Requirement R1, Part 1.3.

Control Center Ownership

The standard requirements address protection for Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers owned by a single Responsible Entity. They also cover the applicable data transmitted between Control Centers owned by two or more separate Responsible Entities. Unlike protection between a single Responsible Entity's Control Centers, applying protection between Control Centers owned by more than one Responsible Entity requires additional coordination. The requirements do not explicitly require formal agreements between Responsible Entities partnering for protection of applicable data. It is strongly recommended, however, that these partnering entities develop agreements, or use existing ones, to define responsibilities to ensure the security objective is met. An example noted in FERC Order No. 822 Paragraph 59 is, "if several registered entities have joint responsibility for a cryptographic key management system used between their

respective Control Centers, they should have the prerogative to come to a consensus on which organization administers that particular key management system."

As an example, ~~the reference model below~~Figure 5 shows several~~some of the~~ data transmissions between Control Centers that a Responsible Entity should consider to be in-scope. The example does not include all possible scenarios. The solid green lines are in-scope communications and~~.~~ ~~T~~the dashed red lines are out-of-scope communications.

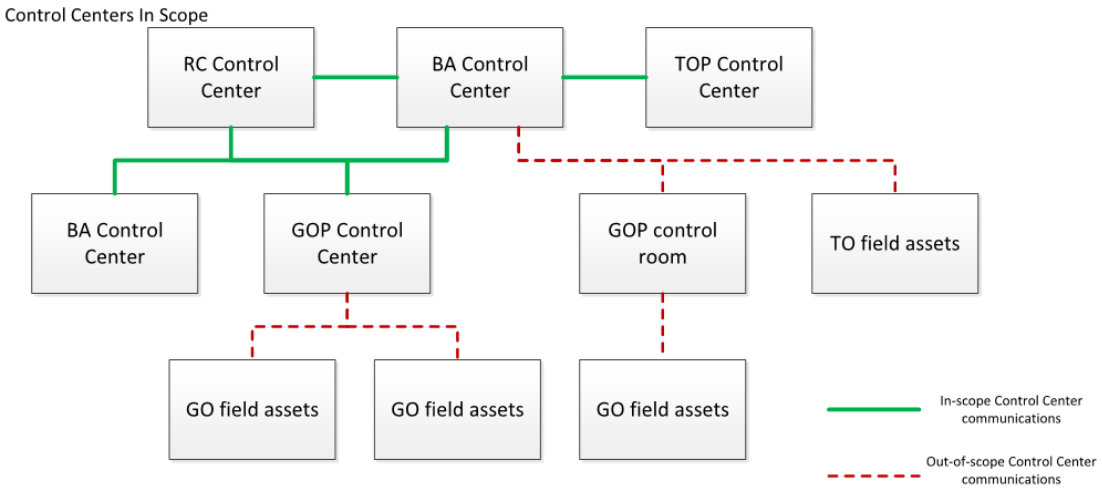


Figure 5: This reference model is an example and does not include all possible scenarios.

The SDT included ~~p~~Part 1.3 of the plan to address the situation when multiple registered entities are involved with protecting the data transmitted between Control Centers. Part 1.3 provides a mechanism to specify which entity is responsible for the application of security controls. The SDT included this requirement part to address security concerns as well as audit concerns. Where data is transmitted between different entities, the SDT asserts that it is necessary for both entities to understand the responsibilities of applying security controls to ensure the data is protected through its entire transmission and there is no security gap. The SDT also asserts this requirement part will provide evidence which may prevent the simultaneous auditing of multiple entities for each communication link between Control Centers when operated by different Responsible Entities. Security controls applied by the entity to achieve compliance with ~~p~~Parts 1.1 and 1.2 of the plan should correlate to the documented responsibilities in ~~p~~Part 1.3 of the entity's plan.

References

Here are several references to assist entities in developing plan(s) for protection of communication links:

- NIST Special Publication 800-53A, Revision 4: Security and Privacy Controls for Federal Information Systems and Organizations
- NIST Special Publication 800-82: Guide to Industrial Control Systems (ICS) Security
- NIST Special Publication 800-175B: Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms
- NIST Special Publication 800-47: Security Guide for Interconnecting Information Technology Systems

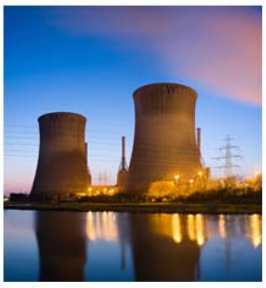
NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DRAFT Implementation Guidance
Pending Submittal for ERO Enterprise Endorsement

Cyber Security – Communications Between Control Centers

Implementation Guidance for CIP-012-1

RELIABILITY | ACCOUNTABILITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Introduction

The Project 2016-02 SDT drafted this Implementation Guidance to provide example approaches for compliance with CIP-012-1. Implementation Guidance does not prescribe the only approach, but highlights one or more approaches that would be effective in achieving compliance with the standard. Because Implementation Guidance only provides examples, entities may choose alternative approaches that better fit their individual situations[1].

Responsible Entities may find it useful to consider this Implementation Guidance document along with the additional context and background provided in the SDT-developed Technical Rationale and Justification for CIP-012-1 document.

Background

The Commission issued Order No. 822 on January 21, 2016. Order 822 approving seven CIP Reliability Standards and new or modified definitions, and directed modifications be made to the CIP Reliability Standards. Among other items, the Commission directed NERC to "develop modifications to the CIP Reliability Standards to require responsible entities to implement controls to protect, at a minimum, communication links and sensitive bulk electric system data communicated between bulk electric system Control Centers in a manner that is appropriately tailored to address the risks posed to the bulk electric system by the assets being protected (i.e., high, medium, or low impact)." (Order 822, Paragraph 53)

In response to the directive in Order No. 822, the Project 2016-02 standard drafting team (SDT) drafted Reliability Standard CIP-012-1 to require Responsible Entities to implement controls to protect sensitive Bulk Electric System (BES) data and communications links between BES Control Centers. Due to the sensitivity of the data being communicated between Control Centers, the standard applies to all impact levels (i.e., high, medium, or low impact).

The SDT drafted requirements to provide Responsible Entities the latitude to protect the communication links, the data, or both, to satisfy the security objective consistent with the capabilities of the Responsible Entity's operational environment.

[1] NERC's Compliance Guidance Policy

Requirements

R1. *The Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) to mitigate the risks posed by unauthorized disclosure and unauthorized modification of Real-time Assessment and Real-time monitoring data while being transmitted between any applicable Control Centers. The Responsible Entity is not required to include oral communications in its plan. The plan shall include: [Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. Identification of security protection used to mitigate the risks posed by unauthorized disclosure and unauthorized modification of Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers;

1.2. Identification of where the Responsible Entity applied security protection for transmitting Real-time Assessment and Real-time monitoring data between Control Centers; and

1.3. If the Control Centers are owned or operated by different Responsible Entities, identification of the responsibilities of each Responsible Entity for applying security protection to the transmission of Real-time Assessment and Real-time monitoring data between those Control Centers.

General Considerations

Plan Development

As noted in the Technical Rationale and Justification for CIP-012-1, the focus of Requirement R1 is implementing a documented plan to protect information that is critical to the real-time operations of the Bulk Electric System while in transit between applicable Control Centers. The number of plan(s) and their content may vary depending on a Responsible Entity's management structure and operating conditions. The Responsible Entity may document as many plans as necessary to meet its needs. For instance, a Responsible Entity may choose to document one plan per Control Center or choose an all-inclusive, single plan for its Control Center communication environment. A Responsible Entity may choose to document one plan for communications between Control Centers it owns and a separate plan for communications between its Control Centers and the Control Centers of a neighboring Entity. The number and structure of the plans is at the discretion of the Responsible Entity as long as the plan(s) include the required elements described in Parts 1.1, 1.2, and 1.3 of Requirement R1.

Identification of Real-time Assessment and Real-time monitoring data

Responsible Entities can expect to receive or have received requests for Operations Planning Analysis, Real-time Assessment and Real-time monitoring data from their RC(s), BA(s) and TOP(s). These data requests, pursuant to the data specification from TOP-003 and IRO-010 requirements, may also include other types of data under the same request. CIP-012 requires protection only for Real-time Assessment and Real-time monitoring data. If the provided data specification does not indicate which data is Real-time Assessment and Real-time monitoring data, Responsible Entities could choose to conduct an assessment to identify this data from among the other data requested or being communicated. Once a data assessment is completed, the Responsible Entity should confirm its findings with the other communicating entity before applying security controls. If the Real-time Assessment and Real-time monitoring data is not clearly identified in the provided data specification, the Responsible Entity should document the methodology used and all actions taken to identify the Real-time Assessment and Real-time monitoring data.

Identification of Security Protection

Entities have latitude to identify and choose which security protection is used to mitigate the risks posed by unauthorized disclosure and unauthorized modification of Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers.

This security protection could consist of logical protection, physical protection, or some combination of both. To determine security protection, the requirement specifies that it must mitigate the risks posed by unauthorized disclosure and unauthorized modification of applicable data.

Security protection implementation can be demonstrated in many ways. If a Responsible Entity uses physical protection, it may demonstrate implementation through review of an applicable Control Center floor plan with details subsequently confirmed through visual inspection, which identifies the physical security measures in place protecting the communication link. If the Responsible Entity uses logical protection, it may demonstrate implementation through an export of the device configuration which applies the security protection. Alternatively, a Responsible Entity may demonstrate implementation through security control monitoring, using an automated monitoring tool to generate reports on the encryption service used to protect a communications link. Where the operational obligations of an entire communication link, including both endpoints, belong to the Control Center of another Responsible Entity, the Responsible Entity without operational obligations for the communication link may demonstrate compliance by ensuring the communications link endpoint is within its Control Center, which could be limited to including the communication link endpoint within a PSP or where other physical protection is applied.

Identification of Where Security Protection is Applied by the Responsible Entity

A Responsible Entity should consider its environment when identifying where security protections should be applied. One approach is to implement security within the Control Center itself to ensure that data confidentiality and integrity is protected throughout the transmission. The Responsible Entity can identify where security protection is applied using a logical or physical location The application of security in accordance with CIP-012 requirements does not add additional assets to the scope of the CIP Reliability Standards. Locations of applied security protection may vary based on many factors such as impact levels of the Control Center, different technologies, or infrastructures. Where the operational obligations of an entire communication link, including both endpoints, belong to the Control Center of another Responsible Entity, the Responsible Entity without operational obligations for the communication link may demonstrate compliance by ensuring the communications link endpoint is within its Control Center, which could be limited to including the communication link endpoint within a PSP or where other physical protection is applied.

Identification of where a Responsible Entity applies security protection could be demonstrated with a list or a Control Center diagram showing either physical or logical security controls. Physical diagrams may require visual confirmation of these controls. These diagrams or a list could be included within the plan developed for R1. A Responsible Entity could also use labels to identify on-site devices where CIP-012 security protection is applied.

When exchanging data between two entities, if a Responsible Entity only manages one end of a communication link, the Responsible Entity is not responsible for identifying where the security protection is applied by the neighboring entity with which it is exchanging data. However, if a Responsible Entity has taken responsibility for both ends of the communication link (such as by placing a router within the neighboring entity's data center), then the Responsible Entity shall identify where the security protection is applied at both ends of the link.

Similarly, if a Responsible Entity owns and operates both Control Centers which are exchanging data (such as in the case of a primary and backup Control Center), then the Responsible Entity shall identify where security protection is applied at both ends of the link.

Identification of Responsibilities when the Control Centers are Owned or Operated by Different Responsible Entities

The Technical Rationale and Justification for CIP-012-1 identifies key considerations in the Control Center Ownership section when communications between Control Centers with different owners or operators. Many operational relationships between Responsible Entities are unique. Consequently, there is no single way to identify responsibilities for applying security protection to the transmission of Real-time Assessment and Real-time monitoring data between Control Centers.

Implementation of responsibilities could also be demonstrated in many ways. Some examples include a joint procedure, a memorandum of understanding, or meeting minutes between the two parties where responsibilities are defined. These responsibilities should be included in both Responsible Entities' plans satisfying requirement Part 1.3.

Where the operational obligations of an entire communication link, including both endpoints, belong to the Control Center of another Responsible Entity, the Responsible Entity without operational obligations for the communication link may demonstrate compliance by ensuring the communications link endpoint is within its Control Center, which could be limited to including the communication link endpoint within a PSP or where other physical protection is applied.

Reference Model

For this Implementation Guidance, the SDT uses a basic reference model of Primary and Backup Control Centers (Entity Alpha) to illustrate approaches to demonstrating compliance. These Control Centers communicate to each other and to a neighboring entity's Control Center (Entity Beta) in configurations outlined by the diagrams in this section. The SDT recognizes that the reference model does not contain many of the complexities of a real Control Center. For this Implementation Guidance, the registration or functions performed in the reference model Control Center are also not considered. A high level block diagram of the basic reference model is shown below in Figure 1. This Implementation Guidance is developed from the perspective of Entity Alpha.

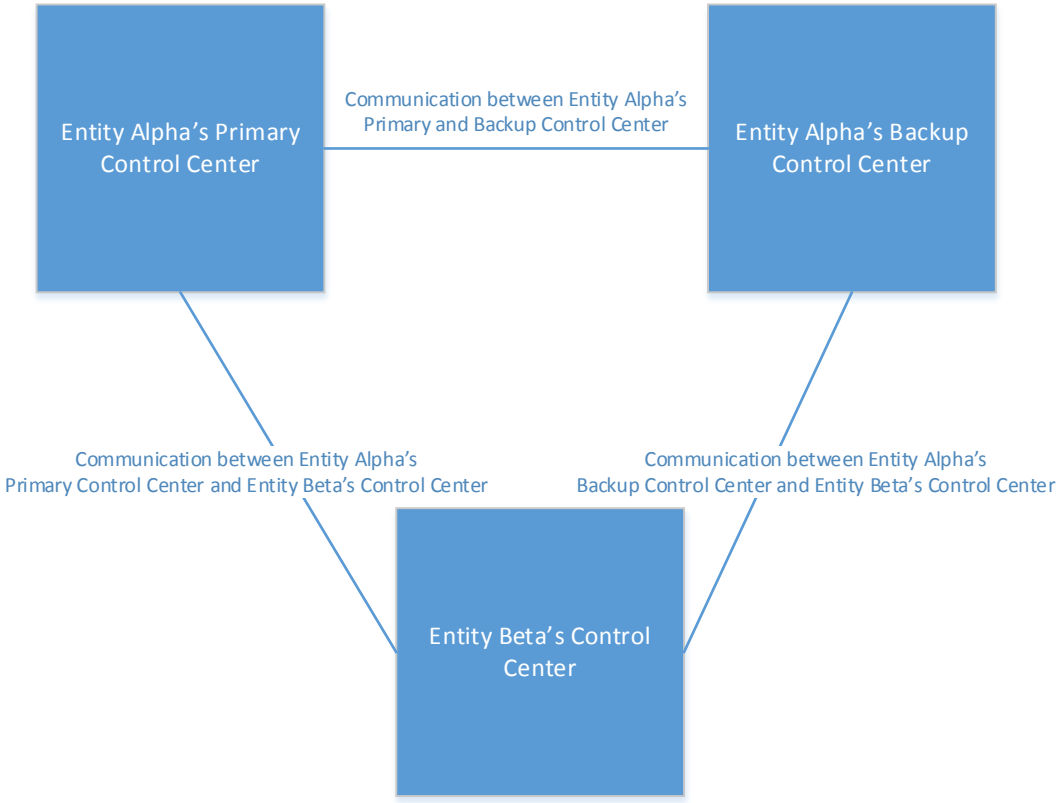


Figure 1: High Level Block Diagram of Reference Model Control Centers

Reference Model Discussion

Requirement R1 requires the implementation of a documented plan. To comply with requirement R1, one approach to a plan is to first determine which communications are in scope of CIP-012-1. There are multiple ways to identify an entity's scope in R1. For example, Entity Alpha in the reference model may first identify the Control Centers with which it communicates. Entity Alpha would determine that there are three: Entity Alpha's Primary Control Center, Entity Alpha's Backup Control Center, and Entity Beta's Control Center. Entity Alpha does not need to consider whether Entity Beta further shares its data with another Entity. That is the responsibility of Entity Beta and is outside of Entity Alpha's purview. Additionally, Entity Alpha does not need to consider any communications to other non-Control Center facilities such as generating plants or substations. These communications are out of scope for CIP-012-1.

Now that Entity Alpha has identified the Control Centers with which it communicates, Entity Alpha identifies either: (1) the Real-time Assessment and Real-time monitoring data; or (2) communication links which are used to transmit Real-time Assessment and Real-time monitoring data between Control Centers. In either case, Entity Alpha should refer to the data specification for Real-time Assessment and Real-time monitoring data identified in

TOP-003-3 and IRO-010-2. For this reference model scenario, identifying the communication links used to transmit Real-time Assessment and Real-time monitoring data may be the most straightforward approach. Through an evaluation of communication links between Control Centers and an evaluation of how it transmits and receives Real-time Assessment and Real-time monitoring data, Entity Alpha determined that it communicates applicable data between its primary and backup Control Centers across a single communication link. Entity Alpha also determined that it communicates applicable data to and from Entity Beta's Control Center across one of two links that originate from either Entity Alpha's primary or backup Control Center using the Inter-Control Center Communications Protocol (ICCP).

With an identified scope of communications links, Entity Alpha now considers the three required elements of its required communications between Control Centers for its plan.

Identification of Security Protection

- Entity Alpha must ensure that protection is applied where identified in its CIP-012-1 plan. The protection must also meet the security objective of mitigating the risks posed by unauthorized disclosure and unauthorized modification of applicable data while in transit between Control Centers. The identification of security protection could be demonstrated by a network diagram similar to that shown in Figure 2 or Figure 3.
- In a simple case where the security protection is applied sufficiently close to the Control Center, such as within the Physical Security Perimeter of the Control Center, Entity Alpha may use a single security protection method to meet the security objective. For this case, shown in Figure 2, Entity Alpha implements a Virtual Private Network (VPN) connection across a private leased communication circuit for each of its three in-scope communication links. To meet the security objective, Entity Alpha further states that its VPN uses Internet Protocol security (IPsec) with encryption.
- For more complex scenarios, Entity Alpha may need to use a combination of security controls. For instance, in Figure 3, Entity Alpha uses a combination of physical security controls (physical access control) and logical security controls (encrypted communications consistent with the first scenario above) to meet the security objective. The SDT notes that the same technical architecture could exist where the responsibilities of the registered entities are different. Therefore as shown in Figure 2 & 3, in the scenario where entity Alpha owns and operationally manages the communication link and endpoint equipment, Entity Beta is responsible for ensuring the communication endpoint of the communication link is within a Control Center. Entity Beta ensures Entity Alpha's communication link endpoint equipment is within a Control Center by including the communication endpoint within a Control Center PSP. The physical controls for the PSP are described in CIP-006 documentation and do not need to be repeated for this requirement. This satisfies Entity Beta's obligation for Part 1.1 and 1.2.
- While these scenarios are all specific to communication links, it is possible that Entity Alpha and Entity Beta achieve the security objective by applying protection to the data rather than the communication links. In this scenario, the application enabling the data exchange between Control Centers may be capable of applying security controls directly to the data. These security controls mitigate the risks posed by unauthorized disclosure and unauthorized modification of applicable data rather than relying on lower level network services to provide this security. For instance, Entity Alpha and Entity Beta may apply security protection at the application layer by using Secure ICCP to exchange applicable data. According to a report released by Sandia National Labs[2], Secure ICCP provides "data integrity indirectly by providing a cryptographic checksum. Secure ICCP provides data confidentiality by encrypting ICCP data exchanges." Methods other than Secure ICCP could also be used to apply security protection to the data at the application layer.

[2] https://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/19-Secure_ICCP_Integration.pdf

Identification of Where Security Protection is Applied by the Responsible Entity

Similar to the identification of security protection above, the identification of where security protection is applied can also be demonstrated by a network diagram similar to those found in Figures 2 and 3.

- Figure 2 shows the identification where CIP-012-1 security protection is applied for the Entity Alpha reference model when a single encrypted tunnel is used to implement the required protection. Entity Alpha has identified that security protection is applied at each of its Control Centers on the external Ethernet interface on the WAN router. While the diagram depicts where Entity Beta has applied security protection for illustrative purposes, Entity Alpha is not responsible for identifying where Entity Beta has applied security protection.
- In order to understand the application of security protection in context of who controls the communication link, it may be helpful to identify both where CIP-012-1 security protection is applied and the location of the telecommunications carrier (telco) demarcation point. Figure 3 provides such an example where the telco demarcation point may not be within the Control Center and based the facts and circumstances surrounding this scenario, Entity Alpha has implemented a combination of security controls to comply with CIP-012-1. In this scenario, Entity Alpha identifies that it has applied physical security protection for its PSP and continuing for its WAN router and that it has applied logical security protection (encryption) at the WAN router. Entity Alpha has also identified the telco demarcation point at a point in the telecommunications cabling connecting to Entity Alpha's WAN router, perhaps at a punch down block for example. In Figure 3, the telco demarcation point is inside the same room as the WAN router. The telco demarcation points are referenced in the drawing for clarity, but are not part of the plan.
- Figures 2 & 3 provide an example of where the operational obligations of an entire communications link, including both endpoints, belong to Entity Alpha. In this case, Entity Beta may be responsible for ensuring the communications endpoint of the communications link is within their Control Center. Entity Beta ensures Entity Alpha's communication link endpoint equipment is within a Control Center by including the communication endpoint within a Control Center PSP. The documentation provided for Part 1.1 by Entity Beta fulfils this obligation.
- The data-centric scenario described above is less intuitive for identifying where security protection is applied by Entity Alpha. If security protection is applied at the application layer (such as Secure ICCP), Entity Alpha could reasonably identify the application or service applying the security (such as the Secure ICCP service) as the location of where security protection is applied.

Identification of Responsibilities when the Control Centers are Owned or Operated by Different Responsible Entities

Entity Alpha and Entity Beta may determine they each are responsible for one end of the VPN configuration on their respective WAN routers. Entity Alpha and Entity Beta have agreed to a 30 character pre-shared key for IPSec authentication.

Rather than use a pre-shared key, Entity Alpha and Entity Beta may decide to use digital certificates for the IPSec authentication using a trusted certificate authority. In that scenario, Entity Alpha and Entity Beta would agree on who is the party responsible for managing the certificate authority.

In the example where the communication link and endpoint equipment are owned by Entity Alpha, both entities should include ownership responsibilities in their plans satisfying requirement 1.3. Examples include but are not limited to, a letter indicating ownership or responsibility, a copy of a contract indicating ownership or responsibilities, an excerpt from an operational agreement or manual indicating ownership or responsibility.

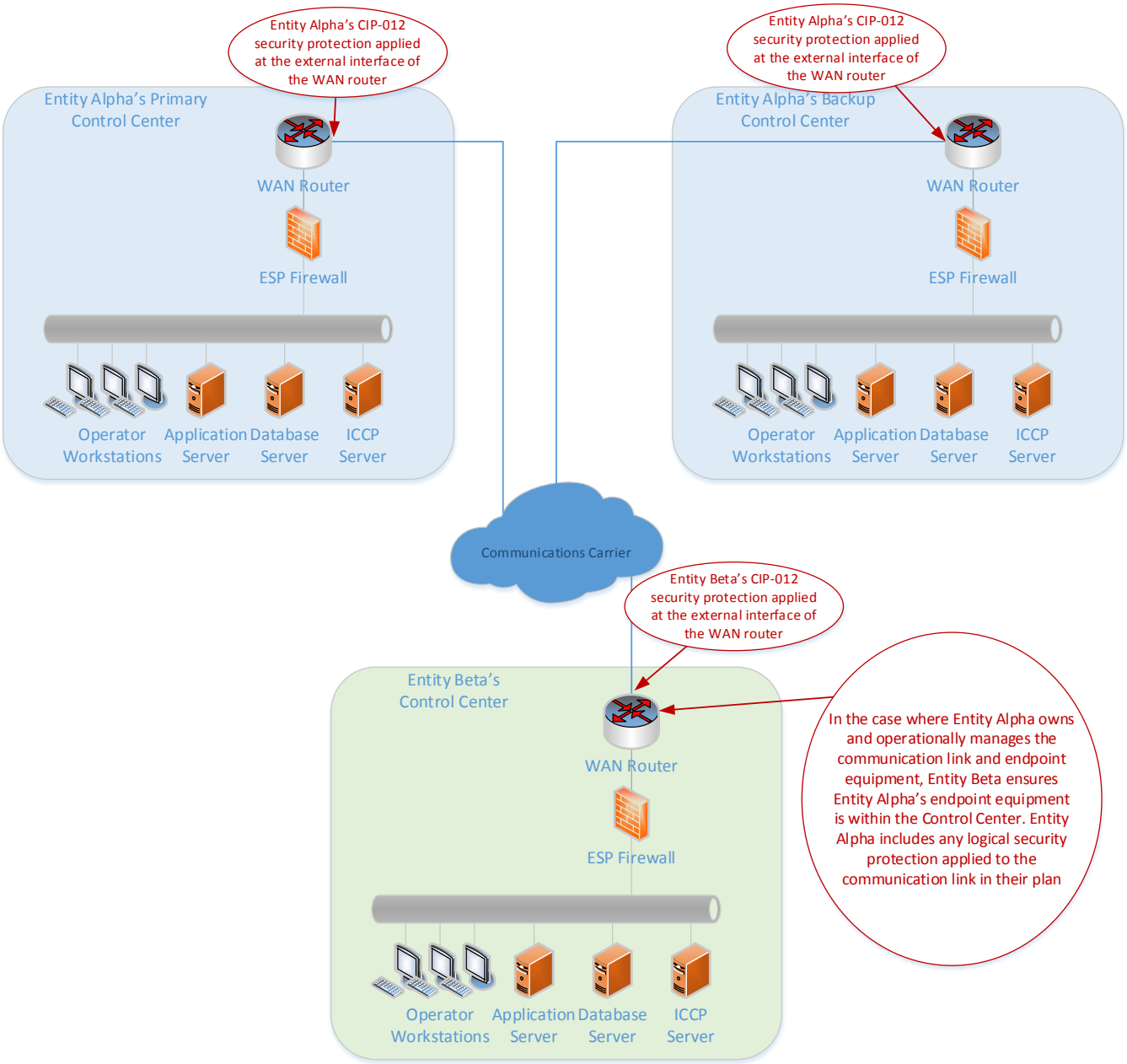


Figure 2: Network diagram and identification of where security protection is applied

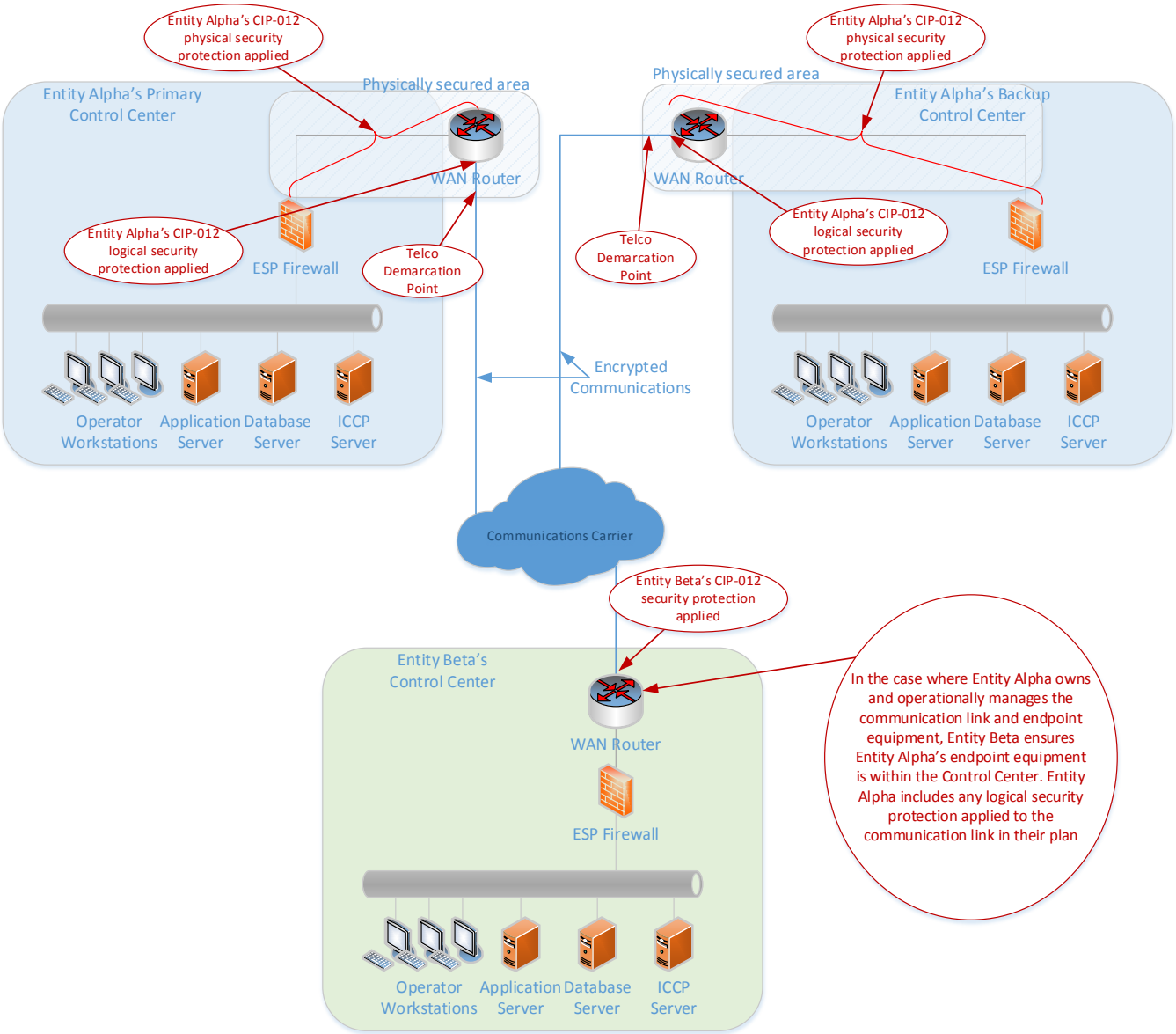


Figure 3: Network diagram using a combination of controls for CIP-012-1

References

Mitre Common Weakness Enumeration (CWE™) list of software weakness types
https://cwe.mitre.org/data/definitions/327.html

Cryptographic Standards and Guidelines
https://csrc.nist.gov/Projects/Cryptographic-Standards-and-Guidelines

NIST Special Publication 800-175B
Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-175B.pdf

Guide to Cryptography
https://www.owasp.org/index.php/Guide_to_Cryptography#Symmetric_Cryptography

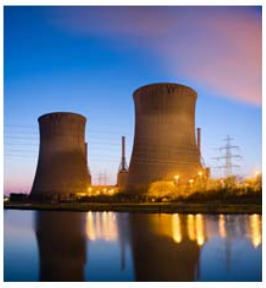
NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DRAFT Implementation Guidance
Pending Submittal for ERO Enterprise Endorsement

Cyber Security – Communications Between Control Centers

Implementation Guidance for CIP-012-1

RELIABILITY | ACCOUNTABILITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Introduction

The Project 2016-02 SDT drafted this Implementation Guidance to provide example approaches for compliance with CIP-012-1. Implementation Guidance does not prescribe the only approach, but highlights one or more approaches that would be effective in achieving compliance with the standard. Because Implementation Guidance only provides examples, entities may choose alternative approaches that better fit their individual situations[1].

Responsible Entities may find it useful to consider this Implementation Guidance document along with the additional context and background provided in the SDT-developed Technical Rationale and Justification for CIP-012-1 document.

Background

The Commission issued Order No. 822 on January 21, 2016. Order 822 approving seven CIP Reliability Standards and new or modified definitions, and directed modifications be made to the CIP Reliability Standards. Among other items, the Commission directed NERC to "develop modifications to the CIP Reliability Standards to require responsible entities to implement controls to protect, at a minimum, communication links and sensitive bulk electric system data communicated between bulk electric system Control Centers in a manner that is appropriately tailored to address the risks posed to the bulk electric system by the assets being protected (i.e., high, medium, or low impact)." (Order 822, Paragraph 53)

In response to the directive in Order No. 822, the Project 2016-02 standard drafting team (SDT) drafted Reliability Standard CIP-012-1 to require Responsible Entities to implement controls to protect sensitive Bulk Electric System (BES) data and communications links between BES Control Centers. Due to the sensitivity of the data being communicated between Control Centers, the standard applies to all impact levels (i.e., high, medium, or low impact).

The SDT drafted requirements to provide Responsible Entities the latitude to protect the communication links, the data, or both, to satisfy the security objective consistent with the capabilities of the Responsible Entity's operational environment.

[1] NERC's Compliance Guidance Policy

Requirements

R1. *The Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) to mitigate the risks ~~of~~ posed by unauthorized disclosure and~~or~~ unauthorized modification of Real-time Assessment and Real-time monitoring data while being transmitted between any applicable Control Centers. The Responsible Entity is not required to include oral communications in its plan. The plan shall include: [Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. Identification of security protection used to mitigate the risks ~~of~~ posed by unauthorized disclosure and~~or~~ unauthorized modification of Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers;

1.2. Identification of where the Responsible Entity applied security protection for transmitting Real-time Assessment and Real-time monitoring data between Control Centers; and

1.3. If the Control Centers are owned or operated by different Responsible Entities, identification of~~y~~ the responsibilities of each Responsible Entity for applying security protection to the transmission of Real-time Assessment and Real-time monitoring data between those Control Centers.

General Considerations

Plan Development

As noted in the Technical Rationale and Justification for CIP-012-1, the focus of Requirement R1 is implementing a documented plan to protect information that is critical to the real-time operations of the Bulk Electric System while in transit between applicable Control Centers. The number of plan(s) and their content may vary depending on a Responsible Entity's management structure and operating conditions. The Responsible Entity may document as many plans as necessary to meet its needs. For instance, a Responsible Entity may choose to document one plan per Control Center or choose an all-inclusive, single plan for its Control Center communication environment. A Responsible Entity may choose to document one plan for communications between Control Centers it owns and a separate plan for communications between its Control Centers and the Control Centers of a neighboring Entity. The number and structure of the plans is at the discretion of the Responsible Entity as long as the plan(s) include the required elements described in ~~p~~Parts 1.1, 1.2, and 1.3 of Requirement R1.

Identification of Real-time Assessment and Real-time monitoring data

Responsible Entities can expect to receive or have received requests for Operations Planning Analysis, Real-time Assessment and Real-time monitoring data from their RC(s), BA(s) and TOP(s). These data requests, pursuant to the data specification from TOP-003 and IRO-010 requirements, may also include other types of data under the same request. CIP-012 requires protection only for Real-time Assessment and Real-time monitoring data. If the provided data specification does not indicate which data is Real-time Assessment and Real-time monitoring data, Responsible Entities could choose to conduct an assessment to identify this data from among the other data requested or being communicated. Once a data assessment is completed, the Responsible Entity should confirm its findings with the other communicating entity before applying security controls. If the Real-time Assessment and Real-time monitoring data is not clearly identified in the provided data specification, the Responsible Entity should document the methodology used and all actions taken to identify the Real-time Assessment and Real-time monitoring data.

Identification of Security Protection

Entities have latitude to identify and choose which security protection is used to mitigate the risks ~~of~~ posed by unauthorized disclosure ~~or~~ and unauthorized modification of Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers.

This security protection could consist of logical protection, physical protection, or some combination of both. To determine security protection, the requirement specifies that it must mitigate the risks posed by~~of~~ unauthorized disclosure ~~or~~ and unauthorized modification of applicable data.

Security protection implementation can be demonstrated in many ways. ~~-~~If a Responsible Entity uses physical protection, it may demonstrate implementation through review of an applicable Control Center floor plan with details subsequently confirmed through visual inspection, which identifies the physical security measures in place protecting the communication link. ~~-~~If the Responsible Entity uses logical protection, it may demonstrate implementation through an export of the device configuration which applies the security protection. Alternatively, a Responsible Entity may demonstrate implementation through security control monitoring, using an automated monitoring tool to generate reports on the encryption service used to protect a communications link. Where the operational obligations of an entire communication link, including both endpoints, belong to the Control Center of another Responsible Entity, the Responsible Entity without operational obligations for the communication link may demonstrate compliance by ensuring the communications link endpoint is within its Control Center, which could be limited to including the communication link endpoint within a PSP or where other physical protection is applied.

Identification of Where Security Protection is Applied by the Responsible Entity

A Responsible Entity should consider its environment when identifying where security protections should be applied. One approach is to implement security within the Control Center itself to ensure that data confidentiality and integrity is protected throughout the transmission. The Responsible Entity can identify where security protection is applied using a logical or physical location The application of security in accordance with CIP-012 requirements does not add additional assets to the scope of the CIP Reliability Standards. Locations of applied security protection may vary based on many factors such as impact levels of the Control Center, different technologies, or infrastructures. Where the operational obligations of an entire communication link, including both endpoints, belong to the Control Center of another Responsible Entity, the Responsible Entity without operational obligations for the communication link may demonstrate compliance by ensuring the communications link endpoint is within its Control Center, which could be limited to including the communication link endpoint within a PSP~~.~~ or where other physical protection is applied.

Identification of where a Responsible Entity applies security protection could be demonstrated with a list or a Control Center diagram showing either physical or logical security controls. Physical diagrams may require visual confirmation of these controls. These diagrams or a list could be included within the plan developed for R1. A Responsible Entity could also use labels to identify on-site devices where CIP-012 security protection is applied.

When exchanging data between two entities, if a Responsible Entity only manages one end of a communication link, the Responsible Entity is not responsible for identifying where the security protection is applied by the neighboring entity with which it is exchanging data. However, if a Responsible Entity has taken responsibility for both ends of the communication link (such as by placing a router within the neighboring entity's data center), then the Responsible Entity shall identify where the security protection is applied at both ends of the link.

Similarly, if a Responsible Entity owns and operates both Control Centers which are exchanging data (such as in the case of a primary and backup Control Center), then the Responsible Entity shall identify where security protection is applied at both ends of the link.

Identification of Responsibilities when the Control Centers are Owned or Operated by Different Responsible Entities

The Technical Rationale and Justification for CIP-012-1 identifies key considerations in the Control Center Ownership section when communications between Control Centers with different owners or operators. Many operational relationships between Responsible Entities are unique. Consequently, there is no single way to identify responsibilities for applying security protection to the transmission of Real-time Assessment and Real-time monitoring data between Control Centers.

Implementation of responsibilities could also be demonstrated in many ways. Some examples include a joint procedure, a memorandum of understanding, or meeting minutes between the two parties where responsibilities are defined. These responsibilities should be included in both Responsible Entities' plans satisfying requirement ~~p~~Part 1.3.

Where the operational obligations of an entire communication link, including both endpoints, belong to the Control Center of another Responsible Entity, the Responsible Entity without operational obligations for the communication link may demonstrate compliance by ensuring the communications link endpoint is within its Control Center, which could be limited to including the communication link endpoint within a PSP or where other physical protection is applied. ~~These responsibilities should be included in both Responsible Entities' plans satisfying requirement part 1.3.~~

Reference Model

For this Implementation Guidance, the SDT uses a basic reference model of Primary and Backup Control Centers (Entity Alpha) to illustrate approaches to demonstrating compliance. These Control Centers communicate to each other and to a neighboring entity's Control Center (Entity Beta) in configurations outlined by the diagrams in this section. The SDT recognizes that the reference model does not contain many of the complexities of a real Control Center. For this Implementation Guidance, the registration or functions performed in the reference model Control Center are also not considered. A high level block diagram of the basic reference model is shown below in Figure 1. This Implementation Guidance is developed from the perspective of Entity Alpha.

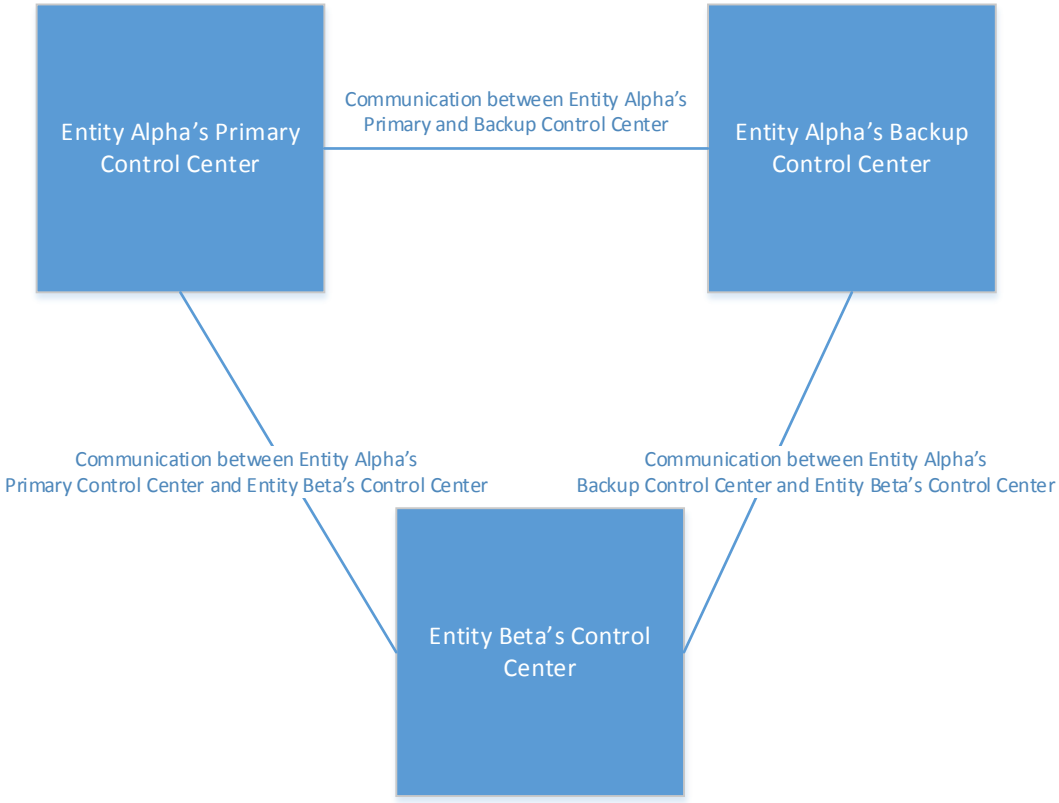


Figure 1: High Level Block Diagram of Reference Model Control Centers

Reference Model Discussion

Requirement R1 requires the implementation of a documented plan. To comply with requirement R1, one approach to a plan is to first determine which communications are in scope of CIP-012-1. There are multiple ways to identify an entity's scope in R1. For example, Entity Alpha in the reference model may first identify the Control Centers with which it communicates. Entity Alpha would determine that there are three: Entity Alpha's Primary Control Center, Entity Alpha's Backup Control Center, and Entity Beta's Control Center. Entity Alpha does not need to consider whether Entity Beta further shares its data with another Entity. That is the responsibility of Entity Beta and is outside of Entity Alpha's purview. Additionally, Entity Alpha does not need to consider any communications to other non-Control Center facilities such as generating plants or substations. These communications are out of scope for CIP-012-1.

Now that Entity Alpha has identified the Control Centers with which it communicates, Entity Alpha identifies either: (1) the Real-time Assessment and Real-time monitoring data; or (2) communication links which are used to transmit Real-time Assessment and Real-time monitoring data between Control Centers. In either case, Entity Alpha should refer to the data specification for Real-time Assessment and Real-time monitoring data identified

in TOP-003-3 and IRO-010-2. For this reference model scenario, identifying the communication links used to transmit Real-time Assessment and Real-time monitoring data may be the most straightforward approach. Through an evaluation of communication links between Control Centers and an evaluation of how it transmits and receives Real-time Assessment and Real-time monitoring data, Entity Alpha determined that it communicates applicable data between its primary and backup Control Centers across a single communication link. Entity Alpha also determined that it communicates applicable data to and from Entity Beta's Control Center across one of two links that originate from either Entity Alpha's primary or backup Control Center using the Inter-Control Center Communications Protocol (ICCP).

With an identified scope of communications links, Entity Alpha now considers the three required elements of its required communications between Control Centers for its plan.

Identification of Security Protection

- Entity Alpha must ensure that protection is applied where identified in its CIP-012-1 plan. The protection must also meet the security objective of mitigating the risks ~~of~~ posed by unauthorized disclosure ~~or~~ and unauthorized modification of applicable data while in transit between Control Centers. The identification of security protection could be demonstrated by a network diagram similar to that shown in Figure 2 or Figure 3.

- In a simple case where the security protection is applied sufficiently close to the Control Center, such as within the Physical Security Perimeter of the Control Center, Entity Alpha may use a single security protection method to meet the security objective. For this case, shown in Figure 2, Entity Alpha implements a Virtual Private Network (VPN) connection across a private leased communication circuit for each of its three in-scope communication links. To meet the security objective, Entity Alpha further states that its VPN uses Internet Protocol security (IPsec) with encryption.

- For more complex scenarios, Entity Alpha may need to use a combination of security controls. For instance, in Figure 3, Entity Alpha uses a combination of physical security controls (physical access control) and logical security controls (encrypted communications consistent with the first scenario above) to meet the security objective. The SDT notes that the same technical architecture could exist where the responsibilities of the registered entities are different. Therefore as shown in Figure 2 & 3, in the scenario where entity Alpha owns and operationally manages the communication link and endpoint equipment, Entity Beta is responsible for ensuring the communication endpoint of the communication link is within a Control Center. Entity Beta ensures Entity Alpha's communication link endpoint equipment is within a Control Center by including the communication endpoint within a Control Center PSP. The physical controls for the PSP are described in CIP-006 documentation and do not need to be repeated for this requirement. This satisfies Entity Beta's obligation for Part 1.1 and 1.2.

- While these scenarios are all specific to communication links, it is possible that Entity Alpha and Entity Beta achieve the security objective by applying protection to the data rather than the communication links. ~~–~~In this scenario, the application enabling the data exchange between Control Centers may be capable of applying security controls directly to the data. These security controls mitigate the risks ~~of~~ posed by unauthorized disclosure ~~or~~ and unauthorized modification of applicable data rather than relying on lower level network services to provide this security. ~~–~~For instance, Entity Alpha and Entity Beta may apply security protection at the application layer by using Secure ICCP to exchange applicable data. ~~–~~According to a report released by Sandia National Labs[2], Secure ICCP provides "data integrity indirectly by providing a cryptographic checksum. Secure ICCP provides data confidentiality by encrypting ICCP data exchanges." Methods other than Secure ICCP could also be used to apply security protection to the data at the application layer.

[2] https://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/19-Secure_ICCP_Integration.pdf

- ~~It is theoretically possible that Entity Alpha and Entity Beta could exchange Real-time Assessment data between Control Centers by email. In that scenario, one approach may be for Entity Alpha to email the applicable data to Entity Beta's Control Center in a protected container such as an encrypted zip file. Entity Alpha and Entity Beta can then exchange the password to that encrypted container through another method, such as by phone. While the notional example of protecting data exchanged by email is a useful illustration of how to achieve the security objective of CIP-012-1, it is extremely unlikely to be used in practice. The characteristics of email communication are inconsistent with the requirements of Real-time data exchange.~~

Identification of Where Security Protection is Applied by the Responsible Entity

Similar to the identification of security protection above, the identification of where security protection is applied can also be demonstrated by a network diagram similar to those found in Figures 2 and 3.

- Figure 2 shows the identification where CIP-012-1 security protection is applied for the Entity Alpha reference model when a single encrypted tunnel is used to implement the required protection. Entity Alpha has identified that security protection is applied at each of its Control Centers on the external Ethernet interface on the WAN router. While the diagram depicts where Entity Beta has applied security protection for illustrative purposes, Entity Alpha is not responsible for identifying where Entity Beta has applied security protection.

- In order to understand the application of security protection in context of who controls the communication link, it may be helpful to identify both where CIP-012-1 security protection is applied and the location of the telecommunications carrier (telco) demarcation point. Figure 3 provides such an example where the telco demarcation point may not be within the Control Center and based the facts and circumstances surrounding this scenario, Entity Alpha has implemented a combination of security controls to comply with CIP-012-1. In this scenario, Entity Alpha identifies that it has applied physical security protection for its PSP and continuing for its WAN router and that it has applied logical security protection (encryption) at the WAN router. Entity Alpha has also identified the telco demarcation point at a point in the telecommunications cabling connecting to Entity Alpha's WAN router, perhaps at a punch down block for example. In Figure 3, the telco demarcation point is inside the same room as the WAN router. The telco demarcation points are referenced in the drawing for clarity, but are not part of the plan.

- Figures 2 & 3 provide an example of where the operational obligations of an entire communications link, including both endpoints, belong to Entity Alpha. In this case, Entity Beta may be responsible for ensuring the communications endpoint of the communications link is within their Control Center. Entity Beta ensures Entity Alpha's communication link endpoint equipment is within a Control Center by including the communication endpoint within a Control Center PSP. The documentation provided for Part 1.1 by Entity Beta fulfils this obligation.

- The data-centric scenario described above is less intuitive for identifying where security protection is applied by Entity Alpha. If security protection is applied at the application layer (such as Secure ICCP), Entity Alpha could reasonably identify the application or service applying the security (such as the Secure ICCP service) as the location of where security protection is applied.

Identification of Responsibilities when the Control Centers are Owned or Operated by Different Responsible Entities

Entity Alpha and Entity Beta may determine they each are responsible for one end of the VPN configuration on their respective WAN routers. Entity Alpha and Entity Beta have agreed to a 30 character pre-shared key for IPSec authentication.

Rather than use a pre-shared key, Entity Alpha and Entity Beta may decide to use digital certificates for the IPSec authentication using a trusted certificate authority. In that scenario, Entity Alpha and Entity Beta would agree on who is the party responsible for managing the certificate authority.

In the example where the communication link and endpoint equipment are owned by Entity Alpha, both entities should include ownership responsibilities in their plans satisfying requirement 1.3. Examples include but are not limited to, a letter indicating ownership or responsibility, a copy of a contract indicating ownership or responsibilities, an excerpt from an operational agreement or manual indicating ownership or responsibility.

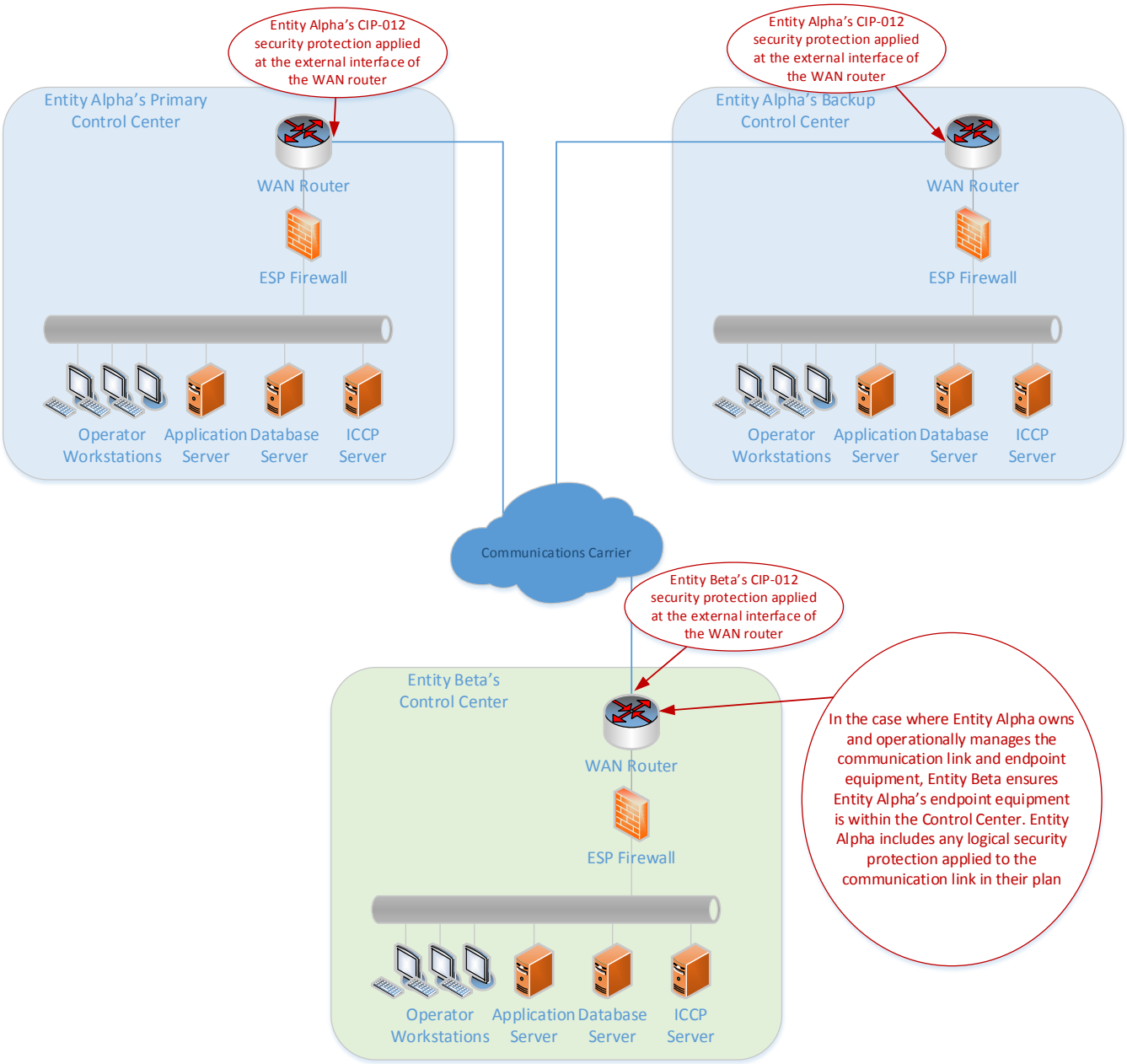


Figure 2: Network diagram and identification of where security protection is applied

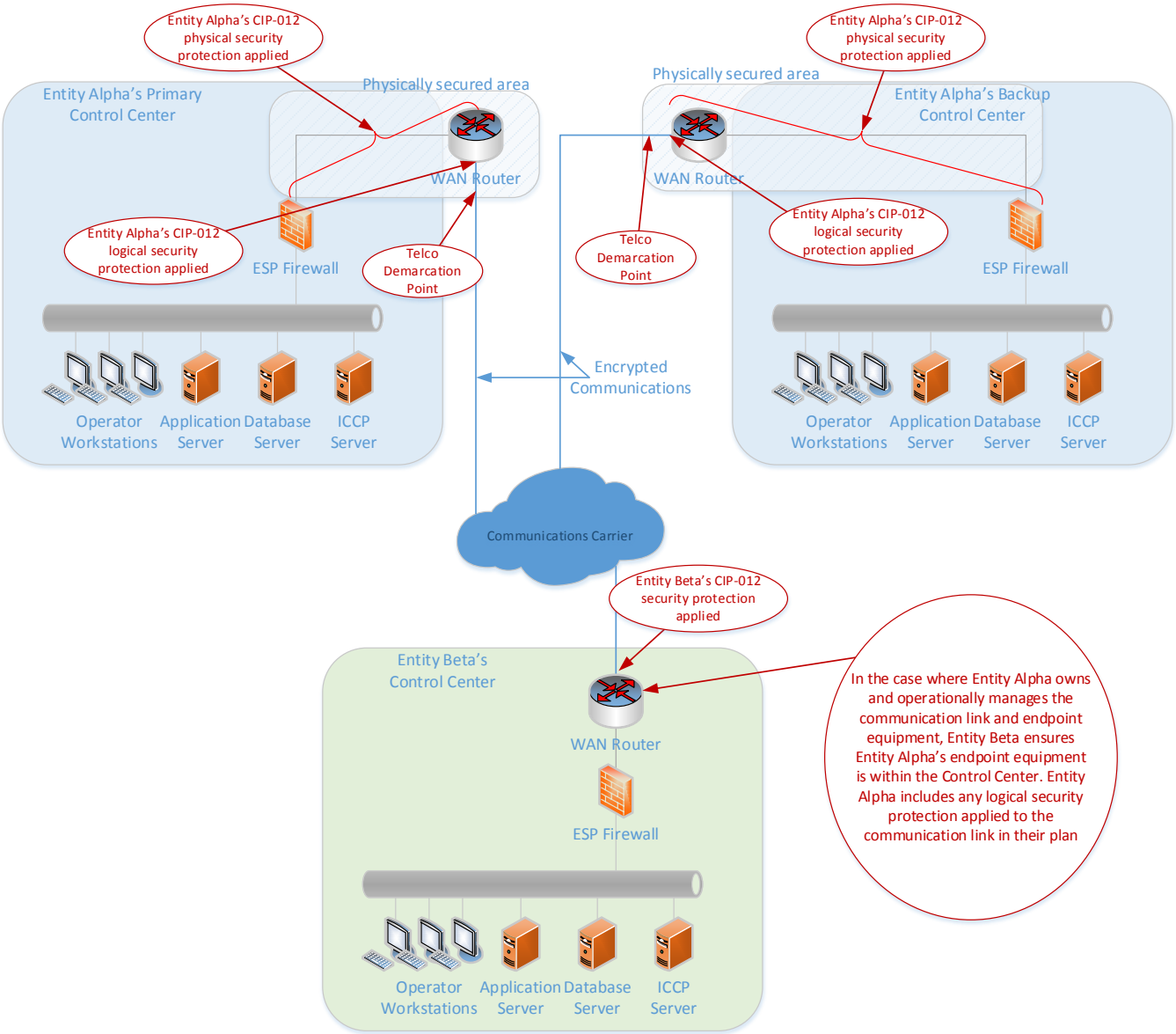


Figure 3: Network diagram using a combination of controls for CIP-012-1

References

Mitre Common Weakness Enumeration (CWE™) list of software weakness types
https://cwe.mitre.org/data/definitions/327.html

Cryptographic Standards and Guidelines
https://csrc.nist.gov/Projects/Cryptographic-Standards-and-Guidelines

NIST Special Publication 800-175B
Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-175B.pdf

Guide to Cryptography
https://www.owasp.org/index.php/Guide_to_Cryptography#Symmetric_Cryptography

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2016-02 Modifications to CIP Standards

Final Ballot Open through August 13, 2018

Now Available

The final ballot for **CIP-012-1 – Cyber Security - Communications between Control Centers** is open through **8 p.m. Eastern, Monday, August 13, 2018.**

Balloting

In the final ballot, votes are counted by exception. Votes from the previous ballot are automatically carried over in the final ballot. Only members of the applicable ballot pools can cast a vote. Ballot pool members who previously voted have the option to change their vote in the final ballot. Ballot pool members who did not cast a vote during the previous ballot can vote in the final ballot.

Members of the ballot pool associated with this project can log in and submit their votes here. If you experience issues navigating the Standards Balloting & Commenting System (SBS), contact Wendy Muller.

- *If you are having difficulty accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out, contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern).*
- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*
- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Next Steps

The voting results will be posted and announced after the ballot closes. If approved, the standard will be submitted to the Board of Trustees for adoption and then filed with the appropriate regulatory authorities.

Standards Development Process

For more information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact Standards Developer, Jordan Mallory (via email) or at (404) 446-2589.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

BALLOT RESULTS

Ballot Name: 2016-02 Modifications to CIP Standards CIP-012-1 FN 5 ST
Voting Start Date: 8/3/2018 10:27:31 AM
Voting End Date: 8/13/2018 8:00:00 PM
Ballot Type: ST
Ballot Activity: FN
Ballot Series: 5
Total # Votes: 252
Total Ballot Pool: 309
Quorum: 81.55
Weighted Segment Value: 72.55

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	80	1	44	0.677	21	0.323	0	3	12
Segment: 2	7	0.6	5	0.5	1	0.1	0	1	0
Segment: 3	73	1	43	0.754	14	0.246	0	3	13
Segment: 4	17	1	9	0.692	4	0.308	0	2	2
Segment: 5	73	1	31	0.608	20	0.392	0	2	20
Segment: 6	46	1	23	0.657	12	0.343	0	3	8
Segment: 7	2	0	0	0	0	0	0	1	1
Segment: 8	3	0.2	2	0.2	0	0	0	0	1
Segment: 9	1	0.1	1	0.1	0	0	0	0	0
Segment: 10	7	0.7	6	0.6	1	0.1	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Totals:	309	6.6	164	4.789	73	1.811	0	15	57

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Affirmative	N/A
1	Allete - Minnesota Power, Inc.	Jamie Monette		Abstain	N/A
1	American Transmission Company, LLC	Douglas Johnson		Affirmative	N/A
1	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	John Shaver		None	N/A
1	Associated Electric Cooperative, Inc.	Ryan Ziegler		Affirmative	N/A
1	Austin Energy	Thomas Standifur		None	N/A
1	Balancing Authority of Northern California	Kevin Smith	Joe Tarantino	Affirmative	N/A
1	Basin Electric Power Cooperative	David Rudolph		None	N/A
1	BC Hydro and Power Authority	Patricia Robertson		Affirmative	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Negative	N/A
1	Bonneville Power Administration	Kammy Rogers-Holliday		Negative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		Negative	N/A
1	Cedar Falls Utilities	Adam Peterson		None	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Hudson Gas & Electric Corp.	Frank Pace		Affirmative	N/A
1	City Utilities of Springfield, Missouri	Michael Buyce		Affirmative	N/A
1	CMS Energy - Consumers Energy Company	James Anderson		Negative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Larry Nash		Affirmative	N/A
1	Duke Energy	Laura Lee		Negative	N/A
1	Edison International - Southern California Edison Company	Steven Mavis		Affirmative	N/A
1	Entergy - Entergy Services, Inc.	Oliver Burke		Affirmative	N/A
1	Eversource Energy	Quintin Lee		Affirmative	N/A
1	Exelon	Chris Scanlon		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A
1	Great Plains Energy - Kansas City Power and Light Co.	James McBee	Douglas Webb	Affirmative	N/A
1	Great River Energy	Gordon Pietsch		None	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Affirmative	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Affirmative	N/A
1	IDACORP - Idaho Power Company	Laura Nelson		Negative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Imperial Irrigation District	Jesus Sammy Alcaraz		None	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Stephanie Burns	Negative	N/A
1	Lincoln Electric System	Danny Pudenz		Negative	N/A
1	Long Island Power Authority	Robert Ganley		Affirmative	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	William Sanders		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Mike Smith		None	N/A
1	MEAG Power	David Weekley	Scott Miller	Affirmative	N/A
1	Memphis Light, Gas and Water Division	Allan Long		None	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Negative	N/A
1	Muscatine Power and Water	Andy Kurriger		Negative	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Affirmative	N/A
1	Nebraska Public Power District	Jamison Cawley		Negative	N/A
1	New York Power Authority	Salvatore Spagnolo		None	N/A
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Affirmative	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Affirmative	N/A
1	Northeast Missouri Electric Power Cooperative	Kevin White		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Negative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Ohio Valley Electric Corporation	Scott Cunningham		Affirmative	N/A
1	Omaha Public Power District	Doug Peterchuck		Negative	N/A
1	Oncor Electric Delivery	Lee Maurer	Tho Tran	Negative	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		Negative	N/A
1	Peak Reliability	Scott Downey		Affirmative	N/A
1	PNM Resources - Public Service Company of New Mexico	Laurie Williams		Affirmative	N/A
1	PPL Electric Utilities Corporation	Brenda Truhe		Affirmative	N/A
1	PSEG - Public Service Electric and Gas Co.	Joseph Smith		Affirmative	N/A
1	Public Utility District No. 1 of Chelan County	Jeff Kimbell		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Long Duong		Abstain	N/A
1	Puget Sound Energy, Inc.	Theresa Rakowsky		Affirmative	N/A
1	Sacramento Municipal Utility District	Arthur Starkovich	Joe Tarantino	Affirmative	N/A
1	Salt River Project	Steven Cobb		Negative	N/A
1	Santee Cooper	Chris Wagner		Negative	N/A
1	SCANA - South Carolina Electric and Gas Co.	Tom Hanzlik		Abstain	N/A
1	Seattle City Light	Pawel Krupa		None	N/A
1	Seminole Electric Cooperative, Inc.	Mark Churilla		None	N/A
1	Sempra - San Diego Gas and Electric	Martine Blair	Jeff Johnson	Affirmative	N/A
1	Sho-Me Power Electric Cooperative	Peter Dawson		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Southern Company - Southern Company Services, Inc.	Katherine Prewitt		Affirmative	N/A
1	Southern Indiana Gas and Electric Co.	Steve Rawlinson		Affirmative	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell		Negative	N/A
1	Tennessee Valley Authority	Howell Scott		Affirmative	N/A
1	Tri-State G and T Association, Inc.	Tracy Sliman		Negative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Negative	N/A
1	Westar Energy	Allen Klassen		Affirmative	N/A
1	Western Area Power Administration	sean erickson		Negative	N/A
1	Xcel Energy, Inc.	Dean Schiro		Affirmative	N/A
2	California ISO	Richard Vine		Abstain	N/A
2	Electric Reliability Council of Texas, Inc.	Brandon Gleason		Affirmative	N/A
2	Independent Electricity System Operator	Leonard Kula		Affirmative	N/A
2	ISO New England, Inc.	Michael Puscas		Affirmative	N/A
2	Midcontinent ISO, Inc.	Terry BIlke		Negative	N/A
2	New York Independent System Operator	Gregory Campoli		Affirmative	N/A
2	PJM Interconnection, L.L.C.	Mark Holman		Affirmative	N/A
3	AEP	Leanna Lamatrice		Affirmative	N/A
3	AES - Indianapolis Power and Light Co.	Bette White		None	N/A
3	APS - Arizona Public Service Co.	Vivian Vo		Affirmative	N/A
3	Arkansas Electric Cooperative Corporation	Mark Gann		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	W. Dwayne Preston		Affirmative	N/A
3	Basin Electric Power Cooperative	Jeremy Voll		Affirmative	N/A
3	BC Hydro and Power Authority	Hootan Jarollahi		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Annette Johnston	Darnez Gresham	Negative	N/A
3	Bonneville Power Administration	Rebecca Berdahl		Negative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City of Farmington	Linda Jacobson-Quinn		Abstain	N/A
3	City of Leesburg	Chris Adkins		None	N/A
3	City of Vero Beach	Ginny Beigel	Brandon McCormick	Negative	N/A
3	City Utilities of Springfield, Missouri	Scott Williams		Affirmative	N/A
3	Cleco Corporation	Michelle Corley	Louis Guidry	Affirmative	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
3	Cowlitz County PUD	Russell Noble		None	N/A
3	Duke Energy	Lee Schuster		Negative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Empire District Electric Co.	Kalem Long		None	N/A
3	Eversource Energy	Sharon Flannery		Affirmative	N/A
3	Exelon	John Bee		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great Plains Energy - Kansas City Power and Light Co.	Jessica Tucker	Douglas Webb	Affirmative	N/A
3	Great River Energy	Brian Glover		Negative	N/A
3	Hydro One Networks, Inc.	Paul Malozewski		None	N/A
3	KAMO Electric Cooperative	Ted Hilmes		Affirmative	N/A
3	Lincoln Electric System	Jason Fortik		Negative	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	Manitoba Hydro	Karim Abdel-Hadi		None	N/A
3	MEAG Power	Roger Brand	Scott Miller	Affirmative	N/A
3	Modesto Irrigation District	Jack Savage	Nick Braden	Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Negative	N/A
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Negative	N/A
3	New York Power Authority	David Rivera	Shelly Dineen	None	N/A
3	NiSource - Northern Indiana Public Service Co.	Aimee Harris		Affirmative	N/A
3	North Carolina Electric Membership Corporation	doug white	Scott Brame	Affirmative	N/A
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Affirmative	N/A
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen		None	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	OTP - Otter Tail Power Company	Wendi Olson		Negative	N/A
3	Owensboro Municipal Utilities	Thomas Lyons		Affirmative	N/A
3	Platte River Power Authority	Jeff Landis		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	PNM Resources - Public Service Company of New Mexico	Lynn Goldstein		Affirmative	N/A
3	Portland General Electric Co.	Angela Gaines		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	Charles Freibert		Affirmative	N/A
3	PSEG - Public Service Electric and Gas Co.	James Meyer		Affirmative	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Puget Sound Energy, Inc.	Tim Womack		Affirmative	N/A
3	Rutherford EMC	Tom Haire		None	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Joe Tarantino	Affirmative	N/A
3	Salt River Project	Robert Kondziolka		Negative	N/A
3	Santee Cooper	James Poston		Negative	N/A
3	SCANA - South Carolina Electric and Gas Co.	Scott Parker		None	N/A
3	Seattle City Light	Tuan Tran		Affirmative	N/A
3	Seminole Electric Cooperative, Inc.	James Frauen		Abstain	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jeff Neas		Affirmative	N/A
3	Silicon Valley Power - City of Santa Clara	Val Ridad		None	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Abstain	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Fred Frederick		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson		Negative	N/A
3	TECO - Tampa Electric Co.	Ronald Donahey		None	N/A
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A
3	Tri-State G and T Association, Inc.	Janelle Marriott Gill		None	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Negative	N/A
3	Westar Energy	Bryan Taggart		Negative	N/A
3	Xcel Energy, Inc.	Michael Ibold		Affirmative	N/A
4	American Public Power Association	Jack Cashin		None	N/A
4	Arkansas Electric Cooperative Corporation	Alice Wright		Affirmative	N/A
4	Austin Energy	Esther Weekes		Affirmative	N/A
4	City of Clewiston	Lynne Mila	Brandon McCormick	Negative	N/A
4	City Utilities of Springfield, Missouri	John Allen		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Aubrey Short		Affirmative	N/A
4	Georgia System Operations Corporation	Andrea Barclay		Affirmative	N/A
4	Indiana Municipal Power Agency	Jack Alvey	Scott Berry	None	N/A
4	National Rural Electric Cooperative Association	Barry Lawson		Affirmative	N/A
4	North Carolina Electric Membership Corporation	John Lemire	Scott Brame	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John Martinsen		Abstain	N/A
4	Sacramento Municipal Utility District	Beth Tincher	Joe Tarantino	Affirmative	N/A
4	Seattle City Light	Hao Li		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Seminole Electric Cooperative, Inc.	Charles Wubbena		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho		Negative	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Negative	N/A
4	WEC Energy Group, Inc.	Anthony Jankowski		Negative	N/A
5	Acciona Energy North America	George Brown		None	N/A
5	AEP	Thomas Foltz		Affirmative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Negative	N/A
5	APS - Arizona Public Service Co.	Kelsi Rigby		Affirmative	N/A
5	Arkansas Electric Cooperative Corporation	Moses Harris		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Brad Haralson		Affirmative	N/A
5	Austin Energy	Shirley Mathew		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	Basin Electric Power Cooperative	Mike Kraft		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Affirmative	N/A
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		Affirmative	N/A
5	Bonneville Power Administration	Scott Winner		Negative	N/A
5	BP Wind Energy North America Inc.	Carla Holly		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Affirmative	N/A
5	Cleco Corporation	Stephanie Huffman	Louis Guidry	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Negative	N/A
5	Colorado Springs Utilities	Jeff Icke		None	N/A
5	Con Ed - Consolidated Edison Co. of New York	William Winters	Alyson Slanover	Affirmative	N/A
5	Dairyland Power Cooperative	Tommy Drea		None	N/A
5	Dominion - Dominion Resources, Inc.	Lou Oberski		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Negative	N/A
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy	Jamie Prater		Affirmative	N/A
5	Exelon	Ruth Miller		Negative	N/A
5	FirstEnergy - FirstEnergy Solutions	Robert Loy		Affirmative	N/A
5	Great Plains Energy - Kansas City Power and Light Co.	Harold Wyble	Douglas Webb	Affirmative	N/A
5	Great River Energy	Preston Walsh		Negative	N/A
5	Gridforce Energy Management, LLC	David Blackshear		None	N/A
5	Hydro-Qu?bec Production	Junji Yamaguchi		None	N/A
5	JEA	John Babik		None	N/A
5	Kissimmee Utility Authority	Mike Blough	Brandon McCormick	Negative	N/A
5	Lakeland Electric	Jim Howard		Negative	N/A
5	Lincoln Electric System	Kayleigh Wilkerson		Negative	N/A
5	Los Angeles Department of Water and Power	Donald Sievertson		Affirmative	N/A
5	Manitoba Hydro	Yuguang Xiao		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Massachusetts Municipal Wholesale Electric Company	David Gordon		Affirmative	N/A
5	MEAG Power	Steven Grego	Scott Miller	Affirmative	N/A
5	Muscatine Power and Water	Neal Nelson		Negative	N/A
5	NB Power Corporation	Laura McLeod		None	N/A
5	Nebraska Public Power District	Don Schmit		Negative	N/A
5	New York Power Authority	Erick Barrios		None	N/A
5	NextEra Energy	Allen Schriver		Affirmative	N/A
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Affirmative	N/A
5	North Carolina Electric Membership Corporation	Robert Beadle	Scott Brame	Affirmative	N/A
5	Northern California Power Agency	Marty Hostler		Negative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	John Rhea		Negative	N/A
5	Omaha Public Power District	Mahmood Safi		Negative	N/A
5	Ontario Power Generation Inc.	David Ramkalawan		Affirmative	N/A
5	OTP - Otter Tail Power Company	Cathy Fogale		Negative	N/A
5	Portland General Electric Co.	Ryan Olson		None	N/A
5	PPL - Louisville Gas and Electric Co.	JULIE HOSTRANDER		Affirmative	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Affirmative	N/A
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Abstain	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Abstain	N/A
5	Puget Sound Energy, Inc.	Eleanor Ewry		Affirmative	N/A
5	Sacramento Municipal Utility District	Susan Oto	Joe Tarantino	Affirmative	N/A
5	Salt River Project	Kevin Nielsen		Negative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Santee Cooper	Tommy Curtis		Negative	N/A
5	SCANA - South Carolina Electric and Gas Co.	Alyssa Hubbard		None	N/A
5	Seattle City Light	Faz Kasraie		None	N/A
5	Seminole Electric Cooperative, Inc.	Brenda Atkins		None	N/A
5	Sempra - San Diego Gas and Electric	Daniel Frank	Andrey Komissarov	None	N/A
5	Silicon Valley Power - City of Santa Clara	Sandra Pacheco		None	N/A
5	Southern Company - Southern Company Generation	William D. Shultz		Affirmative	N/A
5	SunPower	Bradley Collard		None	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin		Negative	N/A
5	Talen Generation, LLC	Matthew McMillan		None	N/A
5	TECO - Tampa Electric Co.	Frank L Busot		None	N/A
5	Tennessee Valley Authority	M Lee Thomas		Affirmative	N/A
5	U.S. Bureau of Reclamation	Wendy Center		Negative	N/A
5	WEC Energy Group, Inc.	Linda Horn		Negative	N/A
5	Xcel Energy, Inc.	Gerry Huitt		Affirmative	N/A
6	APS - Arizona Public Service Co.	Nicholas Kirby		Affirmative	N/A
6	Arkansas Electric Cooperative Corporation	Bruce Walkup		Affirmative	N/A
6	Austin Energy	Andrew Gallo		Affirmative	N/A
6	Basin Electric Power Cooperative	Paul Huettl		Affirmative	N/A
6	Berkshire Hathaway - PacifiCorp	Sandra Shaffer		Negative	N/A
6	Bonneville Power Administration	Andrew Meyers		Negative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Cleco Corporation	Robert Hirchak	Louis Guidry	Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Christopher Overberg		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Affirmative	N/A
6	Duke Energy	Greg Cecil		Negative	N/A
6	Edison International - Southern California Edison Company	Kenya Streeter		None	N/A
6	Entergy	Julie Hall		Affirmative	N/A
6	Exelon	Becky Webb		Negative	N/A
6	FirstEnergy - FirstEnergy Solutions	Ann Ivanc		Affirmative	N/A
6	Florida Municipal Power Pool	Tom Reedy	Brandon McCormick	Negative	N/A
6	Great Plains Energy - Kansas City Power and Light Co.	Jim Flucke	Douglas Webb	Affirmative	N/A
6	Lincoln Electric System	Eric Ruskamp		Negative	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Affirmative	N/A
6	Luminant - Luminant Energy	Brenda Hampton		Abstain	N/A
6	Manitoba Hydro	Blair Mukanik		None	N/A
6	Modesto Irrigation District	James McFall	Nick Braden	Affirmative	N/A
6	Muscatine Power and Water	Ryan Streck		Negative	N/A
6	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		None	N/A
6	NiSource - Northern Indiana Public Service Co.	Joe O'Brien		Affirmative	N/A
6	Northern California Power Agency	Dennis Sismaet		Negative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay		Affirmative	N/A
6	Omaha Public Power District	Joel Robles		None	N/A
6	Portland General Electric Co.	Daniel Mason		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
6	Public Utility District No. 1 of Chelan County	Davis Jelusich		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	LeRoy Patterson		None	N/A
6	Sacramento Municipal Utility District	Jamie Cutlip	Joe Tarantino	Affirmative	N/A
6	Salt River Project	Bobby Olsen		Negative	N/A
6	Santee Cooper	Michael Brown		Negative	N/A
6	Seattle City Light	Charles Freeman		Affirmative	N/A
6	Seminole Electric Cooperative, Inc.	Trudy Novak		Abstain	N/A
6	Snohomish County PUD No. 1	Franklin Lu		Abstain	N/A
6	Southern Company - Southern Company Generation and Energy Marketing	Jennifer Sykes		Affirmative	N/A
6	Southern Indiana Gas and Electric Co.	Brad Lisembee		None	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Rick Applegate		Negative	N/A
6	Talen Energy Marketing, LLC	Jennifer Hohenshilt		None	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Affirmative	N/A
6	WEC Energy Group, Inc.	David Hathaway		Negative	N/A
6	Westar Energy	Megan Wagner	Douglas Webb	Affirmative	N/A
6	Xcel Energy, Inc.	Carrie Dixon		Affirmative	N/A
7	Exxon Mobil	Jay Barnett		None	N/A
7	Luminant Mining Company LLC	Stewart Rake		Abstain	N/A
8	David Kiguel	David Kiguel		Affirmative	N/A
8	Massachusetts Attorney General	Frederick Plett		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
8	Roger Zaklukiewicz	Roger Zaklukiewicz		Affirmative	N/A
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson		Affirmative	N/A
10	Midwest Reliability Organization	Russel Mountjoy		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Affirmative	N/A
10	Northeast Power Coordinating Council	Guy V. Zito		Affirmative	N/A
10	ReliabilityFirst	Anthony Jablonski		Affirmative	N/A
10	SERC Reliability Corporation	Drew Slabaugh		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Affirmative	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Negative	N/A

Previous 1 Next

Showing 1 to 309 of 309 entries

Exhibit I

Standard Drafting Team Roster

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standard Drafting Team Roster

Project 2016-02 Modifications to CIP Standards

	Name	Entity
Co-Chair	David Revill	Georgia System Operations Corporation (GSOC)
Co-Chair	Jay Cribb	Southern Company
Members	Steven Brain	Dominion Energy
	Jake Brown	ERCOT
	Gerald Freese	NIPSCO
	Tom Foster	PJM Interconnection
	Scott Klauminzer	Tacoma Public Utilities, Tacoma Power
	Matthew Hyatt	Tennessee Valley Authority
	Forrest Krigbaum	Bonneville Power Administration
	Heather Morgan	EDP Renewables
	Mark Riley	Calpine
	Abdo Y. Saad	Consolidated Edison Company of New York, Inc.
PMOS Liaisons	Ken Lanehome	Bonneville Power Administration
	Kirk Rosener	CPS Energy
NERC Staff	Jordan Mallory – Standards Developer	North American Electric Reliability Corporation
	Shamai Elstein – Senior Counsel	North American Electric Reliability Corporation
	Marisa Hecht – Counsel	North American Electric Reliability Corporation