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