NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

CIP-012-1

Project 2016-02 Modifications to the CIP Standards: Consideration of Comments

August 2018

RELIABILITY | ACCOUNTABILITY

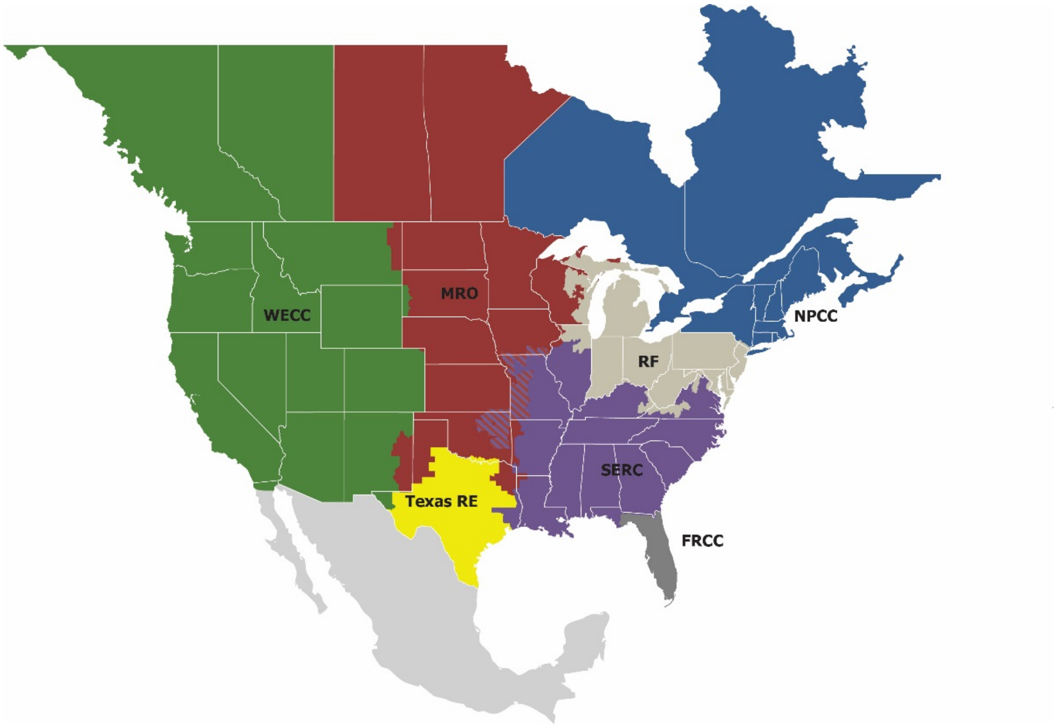
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Preface

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

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



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

Introduction

Background

The Project 2016-02 Modifications to CIP Standards Drafting Team thanks all commenters who submitted comments on the draft CIP-012-1 standard. This standard was posted for a 45-day public comment period through Friday, April 30, 2018. Stakeholders were asked to provide feedback on the standards and associated documents through a special electronic comment form. There were 58 sets of responses, including comments from approximately 155 different people from approximately 108 companies representing the 10 Industry Segments as shown in the table on the following pages.

All comments submitted may be reviewed in their original format on the standard's project page.

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process. If you feel there has been an error or omission, you can contact the NERC standards developer, Jordan Mallory, at 404-446-2589 or at jordan.mallory@nerc.net.

CIP-012-1 Consideration of Comments

Purpose

The Modification to CIP Standards drafting team appreciates industry's comments on the CIP-012-1 standard. The SDT reviewed all comments carefully and made changes to the standard accordingly. The following pages are a summary of the comments received and how the CIP SDT addressed them. If a specific comment was not addressed in the summary of comments, please contact the NERC standards developer.

Control Center Definition

Many commenters expressed concern with the proposed Control Center definition.

The SDT decided to draft exemption language within the applicability section of CIP-012 instead of revising the Control Center definition. Please see the Control Center definition consideration of comments report for additional SDT responses on the new path taken by the SDT.

Control Center

A commenter suggested that the SDT is compounding the Control Center issue by having another explanation of a Control Center/control center to those already present in CIP-002, CIP-014, and the NERC Glossary, and now CIP-012. We recommend a single document that explains the Control Center / control center topic.

The SDT is using this Technical Rationale document to explain its intent in developing the exclusion language in CIP-012-1. The exclusion in CIP-012 is for communications between certain Control Centers and does not modify the definition of Control Center. Use of the Control Center term in other standards is not within the scope of this SDT's SAR.

Control Center Exemption Language

Some commenters provided various examples of language for clarity of the Control Center exemption language within CIP-012. One example of the suggested language and the SDTs response is:

4.2.3 A generating station, Transmission station or substation that is also a Control Center, but meets one of the following criteria:

> **4.2.3.1 Aggregates and transmits Real-time Assessment and Real-time monitoring data from two or more Generation resource(s), Transmission station(s) and/or substation(s) but all aggregated data comes from locations that are contained within the same physical perimeter. (see Figure 1)**
>
> **4.2.3.2 The Control Center does not aggregate and transmit Real-time Assessment and Real-time monitoring data from location(s) outside the physical perimeter where it resides. (see Figure 2)**

The SDT appreciates the included diagrams with Figure 1 and 2 to explain the intent. The SDT asserts that in Figure 1 if an entity defines station at a granular level to where multiple stations are in one "Facility Yard", this would still be considered one "location" and would not fall under the "two or more locations" attribute of the Control Center definition. Since the definition of Control Center uses the term "location", the SDT does not want to introduce a synonymous term of "physical perimeter" and considers the two equivalent.

The SDT also agrees with the scenario depicted in Figure 2. In this scenario, Station 1 could be considered a Control Center depending on the functionality available through the communications to the dual-ported RTUs at other locations. Assuming each separate location is reporting its data to the TOP Control Center with its own individual RTU, that communication is exempted from CIP-012.

Based on these comments, the SDT has created a similar diagram to the ones provided and included it in the Technical Rationale document.

Some commenters recommended the below change along with rationale drafted explaining the reason for the exemption.

A Control Center at a BES generation resource or Transmission station or substation that transmits to another Control Center Real-time Assessment or Real-time monitoring data, such as RTU-style data, pertaining only to the generation resource or Transmission station or substation at which the data transmitting transmitted Control Center is located.

Rationale: The first use of "Control Center" implies that the exemption is for a Control Center to start with. Where it is not a Control Center but a BES facility that transmits data, via an RTU (RTU was added since it plays a pivotal point of intent within the Technical Rational document).

The SDT modified the Technical Rationale document explaining the reason for the Control Center exemption. In addition to the clarifying changes to the Control Center exemption, please see the updated redline that provides clarifying changes in attempt to make the exemption clearer.

A commenter suggests that there could be increases in security risk with repair personnel going into a PSP without knowing all the CIP security requirements for such devices and have in-house personnel escorting the repair personnel during any repair work.

The SDT asserts that such risks are covered under other CIP standards such as CIP-006 and CIP-004.

Requirement R1

A commenter expressed that Real-time Assessments list a number of specific inputs that should be considered for both "Real-time Assessment (RTA) and Real-time monitoring (RTm) data." The commenter suggested there may be an audit approach taken that would require consideration of both RTA AND RTm data for proof that an entity provided adequate protections. The commenter requested that the SDT provide clarification on whether there is a distinction between data used for the RTA and data used for RTm. The commenter recommended consideration of the use of the inputs in the RTA NERC term with a caveat that Entities may choose to protect additional data if they feel the need to expand the scope.

The SDT relied on IRO-010-2 Requirement 1 and TOP-003-3 Requirement R1 that requires RCs, BAs, and TOPs to identify data used for RTA and RTm. The SDT stated in the Implementation Guidance that entities may choose to protect the data, the communication links, or both. The intent is that it may often be easier to identity the communication links over which two Control Centers exchange RTA and RTm data (as well as other data) and protect those communication links which protect all data flowing over them.

Some commenters questioned if CIP Exceptional Circumstance language needed to be added CIP-012-1.

The CIP Exceptional Circumstance language has been added to CIP-012.

A commenter expressed that "security protection used to mitigate risk" is too ambiguous. The commenter requested the SDT consider including two concepts in Requirement R1. The first concept is to clarify whether currently in place ICCP should be encrypted. The commenter noted that the requirement states "while being transmitted between any Control Centers." The commenter further noted that the draft Implementation Guidance has content talking about "both ends of the link" but did not include the expectations for the data while on the

link. The commenter was concerned with latency (primarily for generation control) if secure encryption is expected over the ICCP. Second concept is to include examples that include but are not limiting for security protection.

The SDT asserts that defining a plan to mitigate the risk of modification and disclosure of applicable data allows the Responsible Entity to document the processes that are supportable within its organization and offers flexibility in methods to meet the security objective. The SDT notes that the Implementation Guidance document offers examples of how to comply with the standard.

The SDT encourages Responsible Entities to submit additional scenarios as Implementation Guidance[1] through pre-qualified organizations for endorsement consideration.

Some commenters expressed that CIP-012 is unnecessary and that IRO-010 and TOP-003 already require a mutually agreeable security protocol. Additionally, another commenter expressed concern about the overlap between CIP-012 and TOP-003-3/IRO-010-2. The commenter questioned whether these standards should be combined.

FERC Order No. 822 paragraph 60 recognizes those requirements in IRO-010 and TOP-003 and states the reliability gap to be addressed as “while responsible entities are required to exchange real-time and operational planning data necessary to operate the bulk electric system using mutually agreeable security protocols, there is no technical specification for how this transfer of information should incorporate mandatory security controls.” The modification of these other standards to remove the mutually agreeable security protocol requirement is outside the scope of this team’s SAR.

A commenter requested clarity on the Responsible Entity in charge of securing the data being transmitted from a generator on RC, BA, and TOP equipment. The commenter suggested that the RC, BA, and TOP identify the GOP responsibilities under Part 1.3.

If the Generator is not a Control Center then CIP-012 does not apply as it is only between Control Centers. However, if the Generator is an applicable Control Center, then Requirement R1 Part 1.3 is intended to require the entities to document their responsibilities.

A commenter requested the SDT clarify whether CIP-012-1 applies to low, medium, or high BES Cyber Systems. The commenter requested the SDT also consider how to incorporate the scoping criteria into CIP-002.

The SDT asserts that the applicability is to data being transmitted between Control Centers of all impact levels in response to FERC Order 822 paragraph 58.

Some commenters noted that Real-time monitoring is not a defined term and that the R in Real-time should not be capitalized. In addition, the commenters expressed concern that coordination between Control Centers may result in compromises that may not satisfy the needs of the entities involved.

The term "Monitor" has been lowercased. “Real-time" is defined in the NERC Glossary of Terms and correctly used.

A commenter expressed concern that Operations Planning Analysis (OPA) data is not included in CIP-012-1. In addition, the commenter also noticed the Violation Time Horizon is for Operations Planning. Since the SDT has indicated reasons for excluding OPA data, the commenter asked whether the relevant Violation Time Horizon should be Real-time Operation.

[1] NERC Compliance Guidance Policy: https://www.nerc.com/pa/comp/guidance/Documents/Pre-qualified_org_submittal_with_form.pdf

Please see CIP-012-1 Consideration of Comments Summary Response for the OPA part. Due to the plan being drafted ahead of time; it would not be considered a Real-time Horizon and should remain operations planning horizon.

A commenter disagreed that having a plan adds to the reliability of protecting data used for Real-time Assessment and Real-time monitoring and commented that a plan is not needed. Some commenters recommended replacing the term "plan" with "process" throughout CIP-012-1, the Technical Rationale, Implementation Guidance, and other associated documents. Additionally, some commenters recommended that entities not be required to have a plan in Requirement R1, but have an actionable Requirement to implement. A suggestion was provided.

Based on industry feedback from a prior comment period, the SDT chose a requirement structure that is consistent with many other CIP standards to implement a documented plan. With regard to the use of the "process" instead of "plan", the SDT notes that the term 'documented process' refers to a set of required instructions specific to the Responsible Entity, designed to achieve a specific outcome. The plan to meet R1 may simply include documentation of the required elements of the Parts of CIP-012-1 Requirement R1. The plan also allows for R1 Part 1.3 to document the entities' responsibilities.

A commenter asked whether the current set of standards address those additional vulnerabilities in the entity's IT Security Plan. The commenter suggested that the current plan should be updated to include these additional risks, threats and integrated solution(s) that are already performed by the entity.

The documented plan(s) will need to address the security protection in place to mitigate the risk of unauthorized disclosure and unauthorized modification of applicable data transmitted between any Control Centers in accordance with the specified attributes in the Requirement Parts.

Some commenters questioned whether Requirement 1 Part 1.3 is needed.

Requirement R1 Part 1.3 provides entities a mechanism to specify which entity is responsible for the application of security controls, but not the actual security controls the other entity is responsible for. The SDT believes this is necessary for validation in an audit for an entity to have documented which controls it is responsible for in order to prevent the simultaneous auditing of multiple entities for each communication link between Control Centers operated by different Responsible Entities. Additionally, where data is transmitted between different entities, the SDT asserts that it is necessary for both entities to understand the responsibilities of applying the security controls for the entire transmission in order to ensure that the data is protected. Additional information has been added to the technical rationale document.

Some entities requested additional guidance around the different approaches to mitigating the risk of unauthorized disclosure or modification of data in transit.

The SDT encourages entities to work with prequalified organizations to submit Implementation Guidance for consideration.

A commenter asked if Real-time Data was operational data.

The term Real-time monitoring data was chosen for consistency with the data specification in TOP-003 and IRO-010 standards.

A commenter noted that the "SDT is not specifying the controls used to protect confidentiality and integrity. However, the only method available to achieve the proposed required objective is to implement encryption. FERC Order 822 states on page 39, "it is reasonable to conclude that any lag in communication speed resulting from implementation of protections [encryption technologies] should only be measureable on the order of milliseconds

and, therefore, will not adversely impact Control Center communications," but a commenter asserts this statement only refers to a single data stream. It is unknown what encryption will do when dealing with multiple data streams being transmitted at once, from one to many points, not only to the latency added for the reliable operation of the BES, but also to the computing resources."

The SDT agrees that encryption is a way to mitigate the identified risk and will be widely used as the method to do so, but does not want to be prescriptive due to new and improved technology in the future. The objective is to mitigate the identified risk and may require capacity updates to infrastructure in order to do so.

A commenter requested examples be provided on what a CIP exceptional circumstance would be.

The SDT's intent for including CIP Exceptional Circumstances within CIP-012 is to allow for scenarios where, for reliability reasons, restoration of availability of the data flowing between Control Centers may need to take precedence over temporarily unavailable security controls. For example, if two Control Centers are using encryption that is offloaded onto hardware cards and that encryption hardware fails, or if a key management system fails and numerous entities lose communication, the entities may need to restore the data flow as soon as possible for reliability purposes even if the encryption cannot be restored at the same time.

Implementation Plan

Some commenters stated that the 24-month timeline is not enough and requested the implementation timeline be increased to 36 months or a phased-in approach. Additionally, a commenter acknowledged that the standard and implementation plan are silent on physical security for the equipment being used to provide the data protection. The commenter provided an example of protection for a router that is located in another Entity's facility.

The SDT lengthened the implementation timeline in previous drafts based on industry input, but 24 months has met with widespread industry approval in later comment periods. The SDT concluded that a twenty-four (24) month implementation period is appropriate.

Some commenters noted the difficulty on providing responses to the implementation timeline until the Control Center definition is developed.

The SDT understands the uncertainty associated with CIP-012 if the Control Center definition is also under modification. The SDT attempted to modify the Control Center definition to handle issues brought about by CIP-012's communication scope but based on industry comments has chosen to address those specific communication concerns through an exemption in CIP-012. The Control Center definition remains stable. Please see the Consideration of Comments for the Control Center definition for additional information on the SDT's approach.

Technical Rationale for CIP-012-1

Some entities requested the SDT consider including some statements in the Technical Rationale to address the possibility that data requests made related to TOP-003 and/or IRO-010 include other data that is not Real-time Assessment data or Real-time monitoring data and how the Responsible Entity could exclude this other data from the security requirements.

The SDT agrees and has added a section on this topic to the Technical Rationale document.

A commenter noted that when addressing the security protections, the rationale should include that logical and physical controls can be used. The commenter suggested this should include the team's rationale for allowing these alternatives.

The SDT asserts that the Technical Rationale document already specifies that logical or physical controls can be used to achieve the required security objective.

A commenter noted that the number of regions needs to be updated.

The number of Regions has been updated to reflect the correct number.

Some commenters noted grammatical modifications:

- **In requirement R1 of the technical rationale document, the document should state document plan**
- **The alignment with IRO and TOP standards: last sentence "Real-time Monitoring ", the M should not be capitalized as it is not a NERC defined term.**
- **There appears to be a typo in the footer as it shows Reliability Standard CIP-002-1, instead of CIP-012-1**

The SDT agrees and has made the modifications as noted.

A commenter suggested a clarifying addition to the diagram on page 3 (Control Centers in Scope) of the Technical Rationale document: "In order to make the diagram more closely align to the statement made on page 8 of the Implementation Guidance which states:

'Entity Alpha does not need to consider any communications to other non-Control Center facilities such as generating plants or substations. These communications are out of scope for CIP-012-1.'

The statement above indicates that communications from a Control Center, to a non-Control Center (generation or sub) are out of scope. We suggest that a dotted line be added to the diagram on page 3 (Control Centers in Scope) of the Technical Rational and Justification document to show that communications from a GOP Control Center to a GOP Control Room should be considered out of scope. It is possible that a scenario could exist where GOP Control Centers pass information through a GOP Control Room out to Field Assets."

The SDT asserts that the diagram clearly shows the communications that are in and out of scope. Additionally, this diagram is simply one example and is not inclusive of all possible communication scenarios.

A commenter noted that adding control to the statement "Real-time monitoring" from TOP-003 and IRO-010 may set an expectation that control data will be part of those standards by default. The commenter noted that the proposed CIP-012-1 Implementation Guidance does not use "and control." The commenter recommended that if control is to be part of "Real-time monitoring" then the SDT should make the modifications to all documents, including the Glossary, to reduce misunderstanding.

Based on comments from the prior ballot and comment period, the SDT removed "and control" from the requirement for this posting. The SDT notes that the systems that provide control are generally the same systems that provide monitoring. The SDT removed "and control" to be consistent with the TOP-003 and IRO-010 standards.

A commenter requested that the SDT be consistent with other CIP standards and suggested the SDT combine the Technical Rationale document with the Implementation Guidance document within the draft standard. The commenter also requested the SDT clarify that CIP-012 is a standalone standard that is not associated with all the other CIP standards.

The Technical Rationale document and Implementation Guidance document serve two different purposes. The Technical Rationale document provides the SDT's intent and technical basis for the language in the standard. In addition, the Technical Rationale document provides examples and diagrams to assist entities in understanding the language of the standard. Implementation Guidance is a means for registered entities to develop examples or approaches for ERO Enterprise endorsement to illustrate how registered entities could comply with a standard[2]. There is a project underway reviewing all of the current Technical Rationale documents and removing compliance examples from each document to submit for ERO Enterprise endorsement. Therefore, the Technical Rationale document and Implementation Guidance document cannot be merged together. While the applicability is different from other CIP standards, CIP-012-1 is one standard within the CIP Standard family.

A commenter expressed concern regarding the BCAs and EACMS used for CIP-012-1 may be considered out of scope for the rest of the CIP Reliability Standards based on a statement on Page 6: "The SDT also recognizes that CIP-012 security protection may be applied to a Cyber Asset that is not an identified BES Cyber Asset or EACMS. The identification of the Cyber Asset as the location where security protection is applied does not expand the scope of Cyber Assets identified as applicable under the CIP Cyber Security Standards CIP-002 through CIP-011."

The SDT notes that the assets where the security protection is applied under CIP-012 may be in data transport or telecom equipment that is between discrete ESPs and meet the exclusion in the CIP standards, but still be physically within a Control Center and thus meet the intent of protecting the data while being transmitted between Control Centers. CIP-012-1 neither expands nor diminishes the scope of applicable Cyber Assets under CIP-002 through CIP-011.

Some commenters noted difficulty with implementing Secure ICCP in the past because of concerns over the inability to guarantee a valid certificate at all times.

The SDT asserts that Secure ICCP is an option, but is one option to meeting the objective. The SDT included the flexibility to meet the objective and mitigate the risk at the application, network, or transport layers or even with physical security. Entities are allowed the implementation of physical or logical controls that best meet their operational and reliability needs as long as it meets the security objective specified in CIP-012-1 Requirement R1.

A commenter requested that the SDT provide additional information and a diagram for the scope and exemptions for SCADA data from multiple substations to a remote computer room where data is aggregated at the remote computer room prior to transmitting to a data center that is associated with the Operations Center.

The SDT asserts that CIP-012 provides for the protection of data while being transmitted between Control Centers only and thus excludes communications between Control Centers and field sites such as substations (FERC Order 822, paragraph 57).

A commenter suggested that the SDT provide examples in the Technical Rationale under what circumstances a generating resource or Transmission sub would be applicable to this standard.

The SDT asserts that the standard only applies to generation resources and Transmission substations when those facilities also meet the definition of a Control Center. In all other cases, the standard does not apply to such facilities.

Implementation Guidance

A commenter mentioned that when addressing the security protection that can be used in meeting CIP-012, examples of physical protection should be included in guidance. This should include details on how they can be used to address various parts of the communication between Control Centers.

[2] NERC Compliance Guidance Policy: https://www.nerc.com/pa/comp/guidance/Documents/Pre-qualified_org_submittal_with_form.pdf

The SDT has addressed an example within the implementation guidance document that includes physical protections. Typically physical protection might be used to protect communication links where encryption terminates at a device outside the Control Center in order to protect the data until it arrives inside the Control Center.

A commenter suggested that the last paragraph under Identification of where security protection is applied by the Responsible Entity be split into two separate paragraphs. The commenter suggested the first paragraph would describe how to handle "when exchanging data between two entities" and the second paragraph would focus on "when a Responsible Entity owns and operates both Control Centers."

The SDT agrees with the comment and split the paragraph into two separate paragraphs.

A commenter mentioned that the guidance document is good but until an entity does actual implementation and experiences any issues that arise from the implementation of CIP-012 requirement one can only assume the outcome.

The SDT notes there are a number of ways to demonstrate compliance with the requirement and encourages entities to develop and submit additional examples of Implementation Guidance through pre-qualified organizations for endorsement consideration.

A commenter stated that the implementation of R1.3 will require a standardized solution/technology between entities and a hierarchy of entity responsibilities. The commenter recommended the SDT add guidance and a requirement to identify the entity who is the controlling authority for the secure communications between two or more entities.

The SDT agrees that there will be coordination necessary and designed R1.3 to have the involved entities document those responsibilities. The requirement has been written to allow flexibility on how entities work together on this requirement. The SDT notes there are a number of ways to demonstrate compliance with the requirement and encourages entities to develop and submit additional examples of Implementation Guidance through a pre-qualified organization for endorsement consideration.

Some commenters requested that the SDT define "logical protection" or replace all instances of "logical protection" with "encryption."

The SDT contends that the standard is written to not specify a particular technology. This allows the requirement to be flexible in encompassing future protection solutions.

Some commenters recognized the SDT is not specifying the controls to be used to protect confidentiality and integrity and that the only examples provided in the implementation guidance include encryption. The commenters requested that the SDT provide other methods available to achieve the security objective if they exist. The commenter cited activities and specifications in FERC Order No. 822, such as key management between separate Responsible Entities that must be created and agreed upon by all registered entities involved in the data transfer. The commenter suggested such activities may not be achievable in the 24-month implementation period.

The commenter also noted that a Responsible Entity would lose Real-time Assessment and Real-time monitoring and control data if encryption failed. The commenter suggested a pilot to implement encryption.

The SDT agrees that there will be coordination necessary and designed R1.3 to have the involved entities document the responsibilities. The requirement has been written to allow flexibility on how entities work together on this requirement. The SDT notes there are a number of ways to demonstrate compliance with the requirement and encourages entities to develop and submit additional examples of Implementation Guidance through pre-qualified organizations for endorsement consideration. Please see other comment responses on the 24 month implementation plan. The SDT has included the CIP Exceptional Circumstances language in the requirement in order to allow for encryption failures where reliability may require data to be transferred between Control Centers while the encryption capability is being repaired.

A commenter identified that on page 5 under section "Identification of Where Security Protection is applied by the Responsible Entity", language should be added to address the situation where a Responsible Entity does not manage either end of a communication link, indicating that this Responsible Entity does not have compliance obligations to R1.2.

The SDT agrees and has added such language to clarify obligations in such instances. Requirement 1.3 is also key in the documentation of such cases.

A couple of comments were received that the requirement should be less prescriptive, and additional technical and implementation guidance is needed to provide clarity on the SDT intent and audited scope.

The SDT asserts that the requirement is objective based and describes the risk to be mitigated without prescribing any technical solutions. There are a number of ways to demonstrate compliance with the requirement and the SDT encourages entities to develop and submit additional examples of Implementation Guidance through pre-qualified organizations for endorsement consideration.

Cost Effectiveness

A commenter expressed concern that if the data must be protected throughout the transmission, it would seem that could only be accomplished with encryption. The commenter noted that are cases where the existing equipment is not capable of encryption, replacement will be costly and implementation lengthy. In addition, the commenter stated that due to the large amount of applicable data, access to funds and budget cycle, and resources to perform work required, the solution will be costly.

The SDT has designed CIP-012 with flexibility so the entities can choose the most cost effective means to protect the data while being transmitted between Control Centers. The SDT agrees encryption will be a widely used method and can be accomplished at the application, network, transport, or physical layers or combinations thereof.

Some commenters noted that without clarity on ICCP between Control Centers, the commenters cannot be certain of what is expected, the costs or flexibility.

The SDT notes that data in scope may not be limited to ICCP. This is dependent on the specifics of each entity or entities.

A commenter acknowledged that more flexibility and less guidance could lead to inconsistency on requirement implementation among different entities.

CIP-012 is written to allow for selection of the most practical solution for the entity or entities.

A commenter questioned how the SDT is addressing the scenario where a Responsible Entity identifies multiple types of security protection and one of the forms fails but the data transmission is still protected, meeting the intent of the standard.

In the event of a failure of a protection method, it is the Entity's responsibility to demonstrate how compliance was maintained during the event.

A commenter does not agree the current standard and implementation plan can be executed in a cost effective manner. The commenter noted that encryption has been the only presented solution provided by auditors and SDT guidance to protect both confidentiality and integrity for the data within this scope. The commenter noted that more resources and capital will be required for a 24-month implementation versus a phased-in implementation. The commenter further noted that a phased implementation provides the ability to not only ensure the most effective plan, but also provides the ability to plan more accurately within budget cycles. In addition, the commenter noted that if encryption fails, an entity would lose Real-time Assessment and Real-time monitoring and control data. The commenter expressed concern that a 24-month implementation timeline would impact reliability as there are many opportunities for encryption to fail that must be addressed. The commenter suggested that this has a direct correlation on cost when addressing those opportunities during this timeframe. Additionally, the commenter requested the SDT draft reference models of methods that do not require encryption as a method to protect communications between Control Centers.

CIP-012 is written in a non-prescriptive manner to allow entities to select the protection methods that most appropriately fit their organization. This allows for logical or physical protection as appropriate. Regarding guidance, the SDT encourages entities to draft and submit guidance on other implementation examples.