NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP-012-1

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

May 2018

RELIABILITY | ACCOUNTABILITY



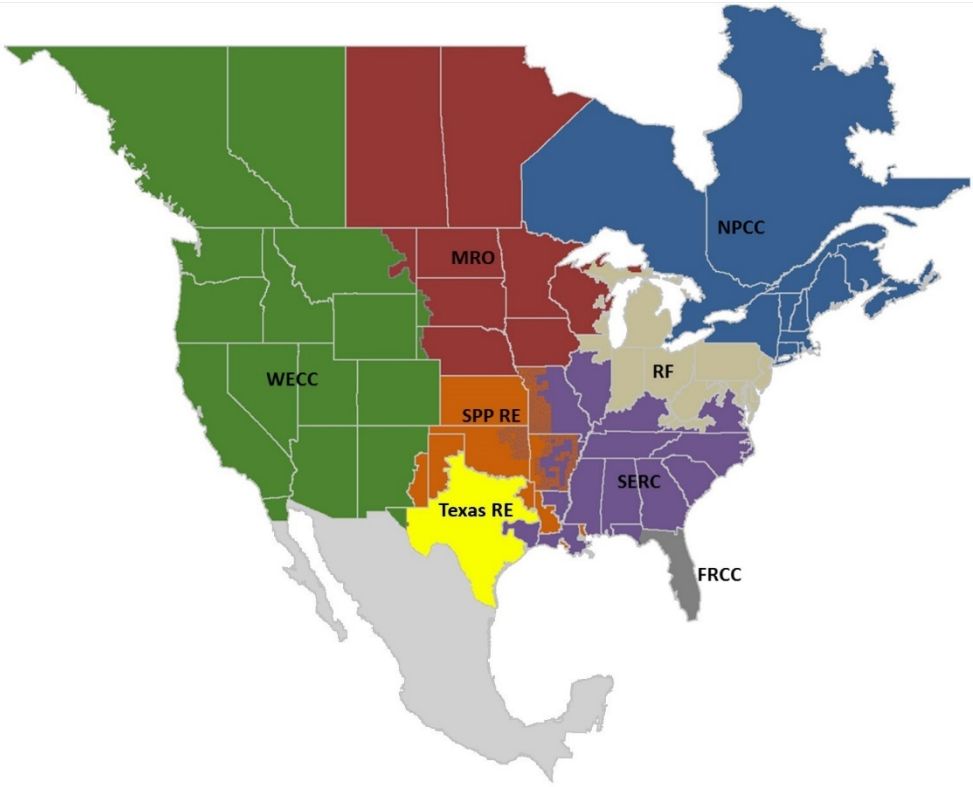

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Preface

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

The North American BPS is divided into eight RE boundaries as shown in the map and corresponding table below.



The North American BPS is divided into eight RE boundaries. The highlighted areas denote overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.

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

Introduction

Background

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

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

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

CIP-012-1 Consideration of Comments

Purpose

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

Control Center Definition

Many commenters expressed concern with the proposed Control Center definition.

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

Requirement R1

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

The TOP-003-3 Requirement R1 already requires TOPs identify data used for RTA and RTm.

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

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

A commenter expressed that "security protection used to mitigate risk" is too ambiguous. The commenter requested the SDT consider including two concepts in Requirement R1. The first concept is to clarify whether currently in place ICCP should be encrypted. The commenter noted that the requirement states "while being transmitted between any Control Centers." The commenter further noted that the draft Implementation Guidance has content talking about "both ends of the link" but did not include the expectations for the data while on the link. The commenter was concerned with latency (primarily for generation control) if secure encryption is expected over the ICCP. Second concept is to include examples that include but are not limiting for security protection.

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

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

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

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

The SDT asserts that the standard is necessary to protect the confidentiality and integrity of applicable data transmitted between Control Centers and is responsive to the directive in Order No. 822.

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

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

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

The SDT asserts that the applicability is clear. It applies to in-scope data being transmitted between Control Centers as defined in the NERC Glossary of Terms and is applicable to all impact levels.

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

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

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

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

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

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

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

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

Implementation Plan

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

The SDT carefully considered all comments and concluded that many factors should be considered to determine an implementation period. These factors include complexity of technology solutions, quantity of telecommunications lines requiring controls and coordination with other Responsible Entities/solution providers, among others. The SDT concluded that a twenty-four (24) month implementation period is appropriate.

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

Please see the Consideration of Comments for the Control Center definition for additional information on the SDT's approach.

Technical Rationale for CIP-012-1

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

The SDT asserts that it is up to the Responsible entity to ensure all RTA and RTm data that is transmitted between Control Centers is protected regardless of whether additional data is also exchanged in regards to the Technical Rationale and the Implementation Guidance Documents.

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

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

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

NERC will make appropriate revisions to various documents upon the effective date of the SPP RE dissolution.

Some commenters noted grammatical modifications:

- **In requirement R1 of the technical rationale document, the document should state document plan**
- **The alignment with IRO and TOP standards: last sentence "Real-time Monitoring ", the M should not be capitalized as it is not a NERC defined term.**

- **There appears to be a typo in the footer as it shows Reliability Standard CIP-002-1, instead of CIP-012-1**

The SDT agrees and will make the modification as noted.

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

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

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

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

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

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

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

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

A commenter expressed concern regarding the BCAs and EACMS used for CIP-012-1 may be considered out of scope for the rest of the CIP Reliability Standards based on a statement on Page 6: "The SDT also recognizes that CIP-012 security protection may be applied to a Cyber Asset that is not an identified BES Cyber Asset or EACMS. The

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

identification of the Cyber Asset as the location where security protection is applied does not expand the scope of Cyber Assets identified as applicable under the CIP Cyber Security Standards CIP-002 through CIP-011."

The SDT notes that the assets where the security protection is applied under CIP-012 may not be part of an entity's identified BCAs or EACMS. If the asset meets the definition of a BCA or EACMS, it should be categorized as such. CIP-012-1 neither expands nor diminishes the scope of applicable Cyber Assets under CIP-002 through CIP-011.

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

The SDT asserts that implementation is not limited to Secure ICCP. Entities are allowed the implementation of physical or logical controls that best meet their operational and reliability needs as long as it meets the security objective specified in CIP-012-1 Requirement R1. This includes the management of certificates.

Implementation Guidance

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

The SDT has addressed an example within the implementation guidance document that includes physical protections.

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

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

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

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

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

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

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

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

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

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

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

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

The SDT notes that the entities communicating the in-scope data are required to have a plan. The plan should specify the responsibilities of the Responsible Entities in protecting the applicable data.

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

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

Cost Effectiveness

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

The 24-month implementation timeline is to allow for selection the most practical solution, as well as for budgeting and acquisition and implementation.

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

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

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

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

A commenter expressed that what is cost effective to some, may not be cost effective to others and questioned the definition of cost effectiveness.

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

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

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

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

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