Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the ~~first~~second draft of the proposed standard.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23 - April 21, 2016
SAR posted for comment	June 1 – June 30, 2016
Informal comment period	February 10- March 13, 2017
45-day formal comment period with additional ballot	July 27 – September 11, 2017
45-day formal comment period with additional ballot	October 27 – December 11, 2017

Anticipated Actions	Date
~~45-day formal comment period with additional ballot~~	~~TBD~~
10-day final ballot	TBD
Board	TBD

~~Upon Board adoption, the rationale boxes will be moved to the Supplemental Material Section.~~

A. Introduction

1. **Title:** Cyber Security – Communications between Control ~~Center Communication Networks~~ Centers

2. **Number:** CIP-012-1

3. **Purpose:** To protect the confidentiality and integrity of Real-time Assessment and Real-time monitoring and control data transmitted between Control Centers ~~required for reliable operation of the Bulk Electric System (BES).~~.

4. **Applicability:**

   4.1. Functional Entities: ~~For the purpose of the~~The requirements ~~contained herein,~~in this standard apply to the following ~~list of~~ functional entities ~~will be collectively,~~ referred to as "Responsible Entities~~." For requirements in this standard where a specific functional entity,~~" that own or ~~subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.~~operate a Control Center.

   4.1.1. Balancing Authority

   4.1.2. Generator Operator

   4.1.3. Generator Owner

   4.1.4. Reliability Coordinator

   4.1.5. Transmission Operator

   4.1.6. Transmission Owner

   4.2. **Exemptions:** The following are exempt from Reliability Standard CIP-012-1:

   4.2.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

   4.2.2. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

5. **Effective Date:** See Implementation Plan for CIP-012-1.

B. Requirements and Measures

~~**Rationale for Requirements R1 and R2:** FERC Order No. 822 directed NERC to develop modifications to the CIP Reliability Standards to require Responsible Entities to implement controls to protect communication links and sensitive Bulk Electric System (BES) data communicated between BES Control Centers. Reliability Standard CIP-012-1 responds to that directive, requiring Responsible Entities to develop a plan to protect the confidentiality and integrity of sensitive data while being transmitted between Control Centers. Responsible~~

~~Entities use various means to communicate information between Control Centers. The plan for protecting these communications is required for all impact levels due to the inter-dependency of multiple impact levels.~~

~~The type of data in scope of CIP-012-1 is data used for Operational Planning Analyses, Real-time Assessments, and Real-time monitoring. The terms Operational Planning Analyses, Real-time Assessments, and Real-time used are defined in the Glossary of Terms Used in NERC Reliability Standards and used in TOP-003 and IRO-010, among other Reliability Standards.~~

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

R1. The Responsible Entity shall develop one or more documented plan(s) to mitigate the risk of ~~the~~ unauthorized disclosure or modification of ~~data used for Operational Planning Analysis,~~ Real-time ~~Assessments,~~Assessment and Real-time monitoring and control data while being transmitted between any Control Centers. This requirement excludes oral communications. The plan shall include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

~~**1.1.** Risk mitigation shall be accomplished by one or more of the following actions:~~

- ~~Physically protecting the communication links transmitting the data;~~
- ~~Logically protecting the data during transmission; or~~

~~**1.2.**~~**1.1.** ~~Using an equally effective method~~Identification of security protection used to mitigate the risk of unauthorized disclosure or modification of ~~the data.~~ Real-time Assessment and Real-time monitoring and control data while being transmitted between Control Centers;

~~Note: If the Responsible Entity does not have a Control Center or it does not transmit the type of data specified in Requirement R1 of CIP-012-1 between two Control Centers, the requirements in CIP-012-1 would not apply to that entity.~~

1.2. Identification of demarcation point(s) where security protection is applied for transmitting Real-time Assessment and Real-time monitoring and control data between Control Centers; and

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

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

R2. The Responsible Entity shall implement the plan(s) specified in Requirement R1, except under CIP Exceptional Circumstances.

M2. Evidence may include, but is not limited to, documentation ~~to demonstrate~~demonstrating implementation of ~~methods to mitigate~~ the ~~risk of the unauthorized disclosure or modification of data in~~plans developed pursuant to Requirement R1.

C. Compliance

1. Compliance Monitoring Process

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

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

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

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

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

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	N/A	~~N/A~~ The Responsible Entity documented its plan(s) but failed to include one of the applicable parts of the plan as specified in Requirement R1.	~~N/A~~The Responsible Entity documented its plan(s) but failed to include two of the applicable parts of the plan as specified in Requirement R1.	The Responsible Entity failed to document ~~one or more~~ plan(s) ~~that achieve the security objective to mitigate the risk of unauthorized disclosure or modification of data used~~ for ~~Operational Planning Analysis, Real-time Assessments, and Real-time monitoring while being transmitted, excluding oral communication, between Control Centers as specified in~~ Requirement R1.
R2.	N/A	N/A	N/A	The Responsible Entity failed to implement its plan(s) ~~to mitigate the risk of unauthorized disclosure or modification of data used for Operational Planning Analysis, Real-time Assessments, and Real-time~~

				~~monitoring while being transmitted, excluding oral communication, between Control Centers~~ as specified in Requirement R1, except under CIP Exceptional Circumstances.

D. Regional Variances

None.

E. Associated Documents

Implementation Plan.

Version History

Version	Date	Action	Change Tracking
1	TBD	Respond to FERC Order No. 822	N/A

Standard Attachments

None.