Standard Development Timeline

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

Description of Current Draft

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

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23 - April 21, 2016
SAR posted for comment	June 1 – June 30, 2016
Informal comment period	February 10- March 13, 2017
45-day formal comment period with ~~additional~~ initial ballot	July 27 – September 11, 2017
45-day formal comment period with additional ballot	October 27 – December 11, 2017
45-day formal comment period with additional ballot	~~TBD~~March 16 – April 30, 2018

Anticipated Actions	Date
45-day formal comment period with additional ballot	May 18 – July 2, 2018
10-day final ballot	~~TBD~~July 30 – August 8, 2018
NERC Board	~~TBD~~August 16, 2018

A. Introduction

1. **Title:** Cyber Security – Communications between Control Centers

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

3. **Purpose:** To protect the confidentiality and integrity of Real-time Assessment and Real-time monitoring ~~and control~~ data transmitted between Control Centers.

4. **Applicability:**

   4.1. Functional Entities: The requirements in this standard apply to the following functional entities, referred to as "Responsible Entities," that own or operate a Control Center.

   4.1.1. Balancing Authority

   4.1.2. Generator Operator

   4.1.3. Generator Owner

   4.1.4. Reliability Coordinator

   4.1.5. Transmission Operator

   4.1.6. Transmission Owner

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

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

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

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

B. Requirements and Measures

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

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

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

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

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

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

~~**M2.** Evidence may include, but is not limited to, documentation demonstrating implementation of the plans developed pursuant to Requirement R1.~~

C. Compliance

1. Compliance Monitoring Process

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

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

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

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

- The Compliance Enforcement Authority ~~(CEA)~~ shall keep the last audit records and all requested and submitted subsequent audit records.

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

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	N/A	The Responsible Entity documented its plan(s) but failed to include one of the applicable parts of the plan as specified in Requirement R1.	The Responsible Entity documented its plan(s) but failed to include two of the applicable parts of the plan as specified in Requirement R1.	The Responsible Entity failed to document plan(s) for Requirement R1;. Or The Responsible Entity failed to implement any Part of its plan(s) for Requirement R1, except under CIP Exceptional Circumstances.
~~**R2.**~~	~~N/A~~	~~N/A~~	~~N/A~~	~~The Responsible Entity failed to implement its plan(s) as specified in Requirement R1, except under CIP Exceptional Circumstances.~~

D. Regional Variances

None.

E. Associated Documents

Implementation Plan.

Version History

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

Standard Attachments

None.