DRAFT

Cyber Security Control Center Communication Plans

Technical Rationale and Justification for Reliability Standard CIP-012-1

August 11, 2017

Table of Contents

Introduction

On January 21, 2016, the Federal Energy Regulatory Commission (FERC or Commission) issued Order No. 822, approving seven Critical Infrastructure Protection (CIP) Reliability Standards and new or modified terms in the Glossary of Terms Used in NERC Reliability Standards, and directing modifications to the CIP Reliability Standards. Among others, the Commission directed the North American Electric Reliability Corporation (NERC) to "develop modifications to the CIP Reliability Standards to require Responsible Entities[1] 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)." (Order 822, Paragraph 53)

In response to the directive in Order No. 822, the Project 2016-02 standard drafting team (SDT) drafted Reliability Standard CIP-012-1 to require Responsible Entities to implement controls to protect sensitive Bulk Electric System (BES) data and communications links between BES Control Centers. Due to the sensitivity of the data being communicated between Control Centers, as defined in the Glossary of Terms Used in NERC Reliability Standards, the standard applies to all impact levels (i.e., high, medium, or low impact).

The SDT drafted requirements to provide Responsible Entities the 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. Requirement R1 requires Responsible Entities to document one or more plans that protect Operational Planning Analysis, Real-time Assessment, and Real-time monitoring data while being transmitted between Control Centers. The plan(s) must address how the Responsible Entity will mitigate the risk of unauthorized disclosure or modification of the applicable data. Requirement R2 covers implementation of the plan developed according to Requirement R1.

This technical rationale and justification document explains the technical rationale for the proposed Reliability Standard to provide stakeholders and the ERO Enterprise an understanding of the technology and technical requirements in the Reliability Standard. It also contains information on the SDT's intent in crafting the requirements.

[1] As used in the CIP Standards, a Responsible Entity refers to the registered entities subject to the CIP Standards.

Requirement R1

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 between Control Centers. This excludes oral communications. [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*
- *Using an equally effective method to mitigate the risk of unauthorized disclosure or modification of the data.*

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.

General Considerations for Requirement R1

The focus of Requirement R1 is on developing a plan to protect information that is critical to the real-time operations of the Bulk Electric System while in transit between applicable Control Centers.

Overview of confidentiality and integrity

The SDT drafted CIP-012-1 to address confidentiality and integrity of data used for Operational Planning Analysis, Real-time Assessment, and Real-time monitoring. This is accomplished by drafting the requirement to mitigate the risk from unauthorized disclosure (confidentiality) or modification (integrity). For this Standard, the SDT relied on the definitions of confidentiality and integrity as defined by National Institute of Standards and Technology (NIST).

- Confidentiality is defined as, “Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.”[2]
- Integrity is defined as, “Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.”[3]

The SDT asserts that the availability of this data is already required by the performance obligation of the Operating and Planning Reliability Standards. The SDT drafted CIP-012 to address the data while being transmitted. The SDT maintains that this data resides within BES Cyber Systems, and while at rest is protected by CIP-003 through CIP-011.

Alignment with IRO and TOP standards

The SDT noted the FERC reference 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 chose to base the CIP-012 requirements 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 entities are required to provide this data under agreements executed with their RC, BA or TOP, often without benefit of knowing how those entities use that data.

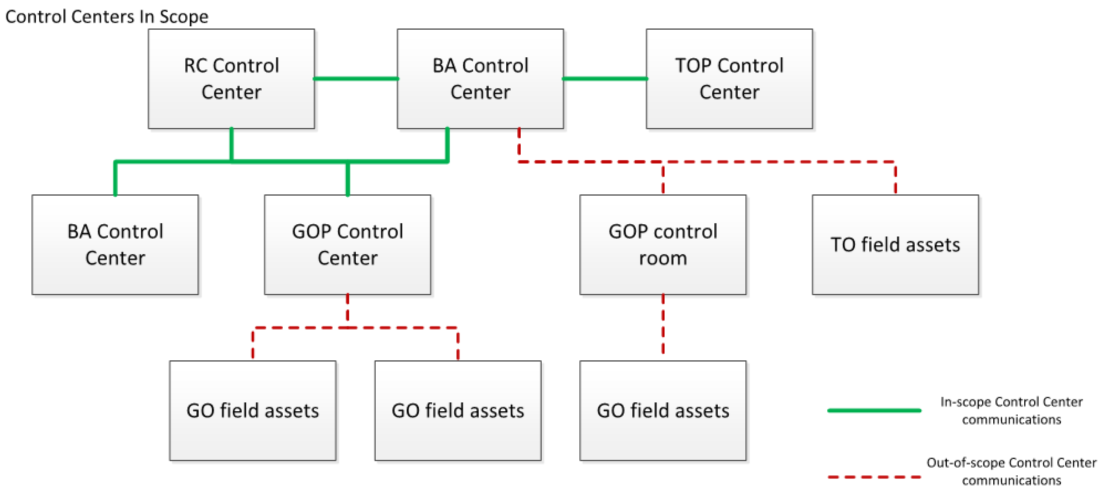
[2] NIST Special Publication 800-53A, Revision 4, page B-3

[3] NIST Special Publication 800-53A, Revision 4, page B-6

Control Center Ownership

The requirements are very clear about implementing protection for data being used for Operational Planning Analysis, Real-time Assessment, and Real-time monitoring while being transmitted between Control Centers owned by a single Responsible Entity. They also cover the applicable data transmitted between Control Centers owned by two or more separate Responsible Entities. Applying protection among a Responsible Entity's owned Control Centers is solely at its discretion. Applying protection between Control Centers owned by more than one Responsible Entity requires additional diligence. The requirements do not explicitly require formal agreements between Responsible Entities partnering for transmission of applicable data. It is strongly recommended, however, that these partnering entities develop agreements, or use existing ones, to define responsibilities to ensure adequate protection is applied. For example as noted in FERC Order No. 822 Paragraph 59, "if several registered entities have joint responsibility for a cryptographic key management system used between their respective Control Centers, they should have the prerogative to come to a consensus on which organization administers that particular key management system." It is important to note that each Responsible Entity may be held individually accountable for the protection applied to the communications methods of data used for Operational Planning Analysis, Real-time Assessment, and Real-time that is transmitted between Control Centers.

As an example, the reference model below depicts some of the data transmissions between Control Centers that a Responsible Entity should consider to be in-scope. The example does not include all possible scenarios. The green solid lines are in-scope communications. The red dashed lines are out-of-scope communications.



Requirement R2

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

General Considerations for R2

The security objective of Requirement R1 can be achieved through a variety of methods or combinations of methods, such as site to site encryption, application layer encryption, physical protection, etc. The protection must prevent unauthorized disclosure or modification of applicable data on the applicable communication methods between Control Centers identified in 1.1. The Responsible Entity has the discretion to choose and apply protection that meets the security objective.

References

Here are several references to assist entities in developing plan(s) for protection of communication links:

- NIST Special Publication 800-53A, Revision 4: Security and Privacy Controls for Federal Information Systems and Organizations
- NIST Special Publication 800-82: Guide to Industrial Control Systems (ICS) Security
- NIST Special Publication 800-175B: Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms
- NIST Special Publication 800-47: Security Guide for Interconnecting Information Technology Systems