DRAFT

Cyber Security – Communications Between Control Centers

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

November 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).

Although the Commission directed NERC to develop modifications to CIP-006, the SDT determined that modifications to CIP-006 would not be appropriate. 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 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.

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 Real-time Assessment and Real-time monitoring and control 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. It will provide stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. It also contains information on the SDT's intent in drafting 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 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 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.

General Considerations for Requirement R1

Requirement R1 focuses 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 Real-time Assessment and Real-time monitoring and control data. This is accomplished by drafting the requirement to mitigate the risk of 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 recognized the FERC reference to additional Reliability Standards and the responsibilities to protect the applicable data in accordance with NERC Reliability 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 Real-time data specification elements 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

The SDT notes that it expanded the phrase “Real-time monitoring” data from TOP-003 and IRO-010 to “Real-time monitoring and control” data. The SDT was concerned that data transmitted between Control Centers that results in the physical operation of BES Elements was not explicitly included in Real-time monitoring data. The SDT understands that in practice Real-time control data is not transmitted separately from Real-time monitoring data. However, the SDT wanted to ensure that Real-time control data was included regardless of whether or not it is transmitted along with Real-time monitoring data. If entities only transmit Real-time control data along with Real-time monitoring data, then the SDT does not intend for such entities to identify additional data beyond that Real-time monitoring data already included in the data specifications for TOP-003 and IRO-010.

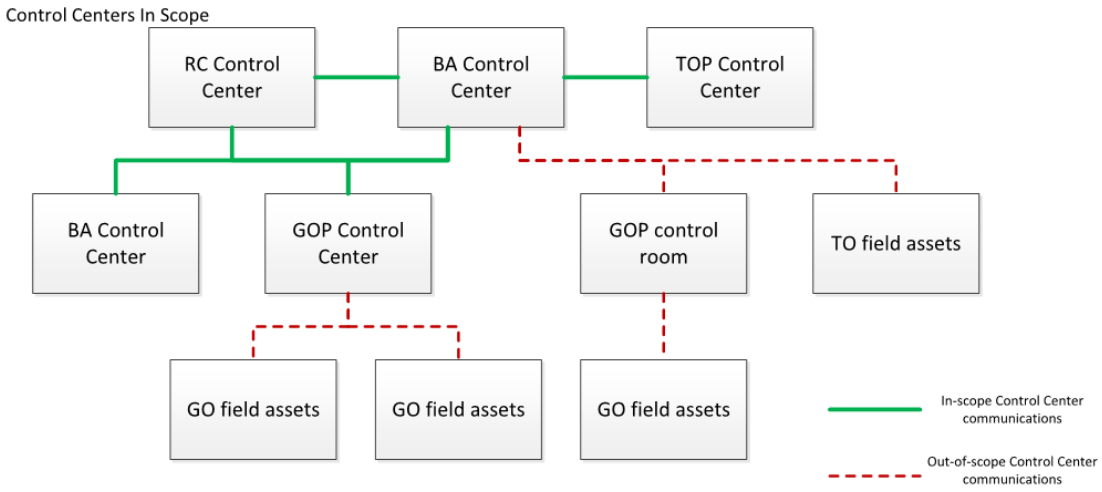
Demarcation Points

The SDT noted the need for an entity to identify a demarcation point inside each Control Center where it will apply protection for applicable data. The SDT used the demarcation point concept for implementing protection to ensure entities could still take advantage of security measures, such as deep packet inspection, already implemented at or near the EAP when ESPs are present, while maintaining the capability to protect the applicable data being transmitted between Control Centers.

Control Center Ownership

The requirements address protection for Real-time Assessment and Real-time monitoring and control data 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. Unlike protection between a single Responsible Entity’s Control Centers, applying protection between Control Centers owned by more than one Responsible Entity requires additional coordination. The requirements do not explicitly require formal agreements between Responsible Entities partnering for protection 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. An example noted in FERC Order No. 822 Paragraph 59 is, “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."

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.



This reference model is an example and does not include all possible scenarios.

Requirement R2

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

General Considerations for R2

Responsible Entities can achieve the security objective of Requirement R1 through a variety of methods or combinations of methods, such as site to site encryption, application layer encryption, physical protection, etc. The protection must be designed to prevent unauthorized disclosure or modification of applicable data on the applicable communication methods between Control Centers identified in Requirement R1.1. The Responsible Entity has the discretion to implement any type of 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