NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Project 2016-02

Modifications to CIP Standards

Consideration of Comments Regarding Implementation Guidance and Technical Rationale and Justification for CIP-012

March 2018

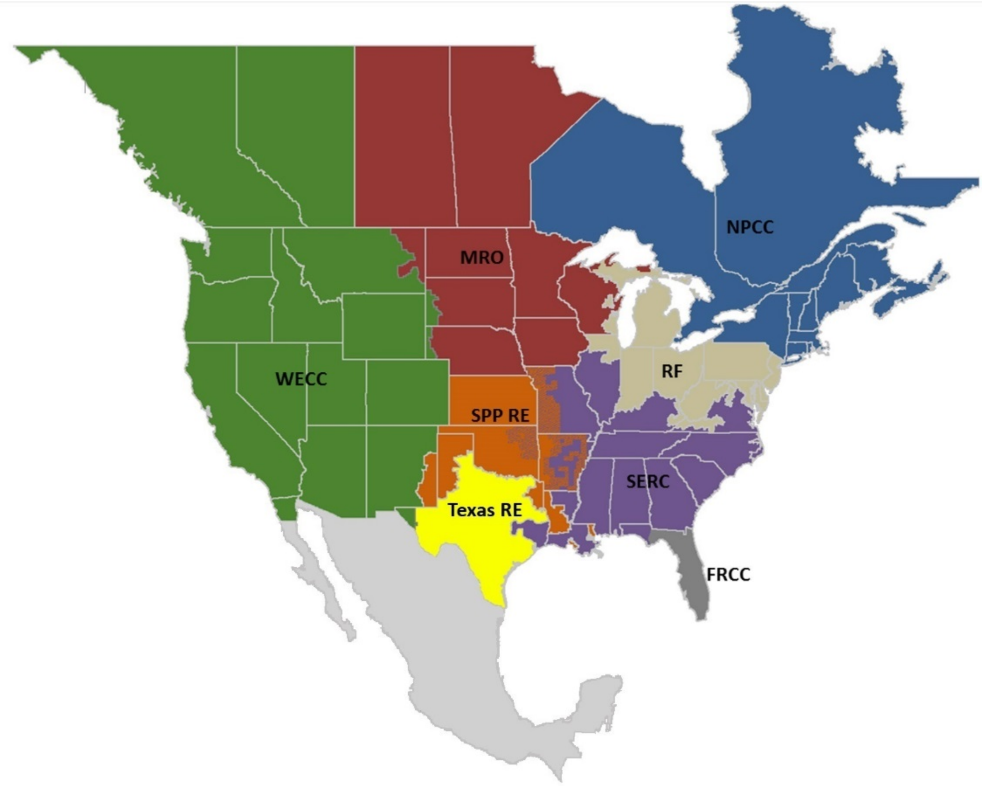
RELIABILITY | ACCOUNTABILITY

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

Preface

The North American Electric Reliability Corporation (NERC) is a not-for-profit international regulatory authority whose mission is to assure the reliability and security of the bulk power system (BPS) in North America. NERC develops and enforces Reliability Standards; annually assesses seasonal and long-term reliability; monitors the BPS through system awareness; and educates, trains, and certifies industry personnel. NERC's area of responsibility spans the continental United States, Canada, and the northern portion of Baja California, Mexico. NERC is the Electric Reliability Organization (ERO) for North America, subject to oversight by the Federal Energy Regulatory Commission (FERC) and governmental authorities in Canada. NERC's jurisdiction includes users, owners, and operators of the BPS, which serves more than 334 million people.

The North American BPS is divided into eight Regional Entity (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

The standard drafting team (SDT) appreciates industry comments on the proposed Implementation Guidance and Technical Rationale and Justification for CIP-012. The SDT considered the comments submitted during the posting of the proposed Implementation Guidance and Technical Rationale and Justification for CIP-012, and adapted its revision approach for the second proposal currently posted. Additionally, the SDT conducted substantial outreach during the revision process, through in-person meetings, conference calls, and stakeholder organization presentations.

On January 21, 2016, the Federal Energy Regulatory Commission (FERC) issued Order No. 822 Revised Critical Infrastructure Protection Reliability Standards. In this order, FERC approved revisions to version 5 of the CIP standards.

Response to Comments

The SDT has carefully reviewed each stakeholder comment and has revised language where suggested changes are consistent with SDT intent and industry consensus. The SDT reviewed and responded to each comment in summary form below.

There were 30 sets of comments, comprised of approximately 84 different people across approximately 59 companies representing 10 of the Industry Segments.

All comments submitted can be reviewed in their original format on the 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 Senior Director of Standards, Howard Gugel (via email) or at (404) 446-9693.

Consideration of Comments – Summary Responses

Implementation Guidance

- Commenters recommended creating a new "BES data" NERC Glossary term to be used to clearly scope the data in question. Commenters also recommended defining the terms "monitoring data" and "control data" in the NERC Glossary.

  The SDT asserts that Real-time monitoring is a well-understood concept that is included in the TOP and IRO standards. Additionally, Real-time Assessment is a defined term within the NERC Glossary of Terms Used in Reliability Standards. Creating new terms and definitions could cause unintended impacts on other standards. The SDT removed "and control" from Requirement R1 and from the Technical Rationale.

- A commenter noted the Technical Rationale and Justification document does not provide any technical implementation guidelines to identify where protections may be applied under the language of the CIP-012-1 standard. The commenter also requested the addition of one or more sample connectivity drawings to the Technical Rationale and Justification document that depict compliant topology configurations showing the R1.1 security protection and R1.2 demarcation point placement that could be applied to an existing pair of in-scope Control Centers, including the associated BCS, ESP (EAP/EACMS), and PSP boundaries.

  The Technical Rationale and Justification document explains the technical rationale for the proposed Reliability Standard. This Technical Rationale and Justification document does not provide examples of how to implement the requirements. However, the SDT has identified physically secure areas and ESP firewalls in the diagrams in the Implementation Guidance for CIP-012-1.

- A commenter recommended the following paragraph from the Technical Rationale and Justification Introduction as it provides an important perspective that appears to not be fully understood. *"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 notes this paragraph is an explanation of the rationale behind developing CIP-012. It does not include information on examples of implementation. The SDT has declined to add this to the Implementation Guidance for these reasons.

- A commenter recommended adding logging to the Identification of Security Protection section on page 7. The commenter also recommended that entities should consider any communications to other non-Control Center facilities such as generating plants or substations. The commenter also suggests including other types of evidence with a floorplan as a floorplan diagram alone would not be sufficient.

  The SDT thanks you for the comments. The SDT notes that the Implementation Guidance is providing a small set of examples of implementation and has aligned the content to the requirement language only. It is not the intent of the SDT to add more rigor in meeting best practice that may be outside the scope of the requirement language. The SDT notes that additional Implementation Guidance documents can be drafted

for any standard. Individual entities are encouraged to work with pre-qualified organizations to submit additional Implementation Guidance for consideration of endorsement by the ERO.

- Commenters requested more examples of technical controls, noting that lack of specifics can cause confusion and lost time. This will aid entities who may decide to implement protection mechanisms that may not be sufficient from a security perspective and then through the course of presentations and guidance have to re-work.

  The SDT thanks you for the comments. The SDT notes that the Implementation Guidance is providing a small set of examples of implementation. SDT notes that additional Implementation Guidance documents can be drafted for any standard. Individual entities are encouraged to work with pre-qualified organizations to submit additional Implementation Guidance for consideration of endorsement by the ERO.

- Commenters noted the Implementation Guidance for CIP-012 does not address non-repudiation and, therefore, integrity as defined by NIST 800-53, Revision 4, page B-6. The commenter requests that the SDT provide additional implementation guidance regarding how the protections are required "…in a manner that reflects the risks posed to bulk electric system reliability," as stated on page 12 of FERC Order No. 822.

  The SDT thanks you for the comments and has removed the example from the Implementation Guidance document.

- Commenters requested that the SDT consider consolidating Requirement R2 into Requirement R1, noting it is unnecessary to have two requirements.

  The SDT agrees with comments regarding a single requirement and has modified Requirement R1 and updated the Implementation Guidance accordingly.

- A commenter noted concerns related to mailbox or virtual RTUs used to communicate data between Control Centers as a redundant method to, or in lieu, of ICCP. Some Entities may forget that such communication could be in-scope of the standard especially if Real-time Assessment and Real-time monitoring and control data is passed through these mailbox or virtual RTUs.

  The SDT thanks you for the comments. As plans are developed, entities should be aware of the various means that data is communicated between Control Centers and account for those means in the plan document(s). The SDT notes that the Implementation Guidance is providing a small set of examples of implementation. SDT notes that additional Implementation Guidance documents can be drafted for any standard. Individual entities are encouraged to work with pre-qualified organizations to submit additional Implementation Guidance for consideration of endorsement by the ERO.

- A commenter noted concerns with the inclusion of "and control" in Requirement R1 and the Implementation Guidance. They also questioned the need to identify roles and responsibilities for applying security protections. They disagreed with including response in considering roles and responsibilities. They also disagreed with specifying an encryption example (AES-128). They also recommended including guidance on agreements with third parties handling data.

  The SDT thanks you for the comments. The SDT notes that the Implementation Guidance is providing a small set of examples of implementation. The SDT intended to provide some specific examples to aid entities. Based on comments, the SDT removed "and control" and "roles" from Requirement R1 and the Implementation Guidance. The SDT contends is it is necessary to document the responsibilities when

communication between Control Centers involves more than one entity and has left "responsibilities" in Requirement R1 and the Implementation Guidance. The SDT removed the specific encryption example from the Implementation Guidance. The SDT removed the example related to third parties from the Implementation Guidance.

- A commenter requested ERO endorsement of the Implementation Guidance before final ballot on CIP-012.

  The SDT thanks you for the comment. The SDT is actively working with NERC staff to coordinate and gain endorsement of the guidance in a timely manner.

- One commenter noted a question of whether communication between a Control Center and associated data centers would be in scope for CIP-012.

  The SDT developed CIP-012 in response to FERC Order 822. Paragraph 58 of FERC Order 822 notes that the requirement "should encompass communication links and data for intra-Control Center and inter-Control Center communications." Through discussions with FERC staff, the SDT came to understand that this paragraph was intended to convey that the requirement should include communications between Control Centers operated by a single entity (such as between a primary and backup Control Center) and communications between Control Centers operated by neighboring entities (such as between a TOP and its RC). The SDT notes that the Control Center by definition includes the associated data center and should, therefore be included with protecting intra-Control Center communications. The SDT did not specify protection for communication within a single Control Center as it did not intend to interfere or cause unintended consequences with the inter-process communications that enable an EMS to function properly.

- A commenter raised questions about data not currently determined to have a 15-minute impact and therefore out of scope for CIP-002 thru CIP-011, e.g. synchrophasers data. The question if this data is out of scope for CIP-012.

  CIP-012 does not use the reference to 15-minute impact. If the data in question is used for Real-time Assessment or Real-time monitoring, the data is in scope for CIP-012.