NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Project 2020-04 Update
Modifications to CIP-012

December 8, 2021

RELIABILITY | RESILIENCE | SECURITY




Agenda

Administrative

- Review NERC Antitrust Compliance Guidelines and Public Announcement

Agenda

- Team Updates
- FERC Order 866
- Standard Updates
- Next Steps
- Questions and Answers

NERC Antitrust

It is NERC's policy and practice to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. This policy requires the avoidance of any conduct that violates, or that might appear to violate, the antitrust laws. Among other things, the antitrust laws forbid any agreement between or among competitors regarding prices, availability of service, product design, terms of sale, division of markets, allocation of customers or any other activity that unreasonably restrains competition. It is the responsibility of every NERC participant and employee who may in any way affect NERC's compliance with the antitrust laws to carry out this commitment.

NERC Public Disclaimer

Participants are reminded that this meeting is public. Notice of the meeting was widely distributed. Participants should keep in mind that the audience may include members of the press and representatives of various governmental authorities, in addition to the expected participation by industry stakeholders.

Standards Drafting Team

	Name	Entity
Chair	Robert Kracke	Southern Company
Vice Chair	Joseph Gatten	Xcel Energy
Members	Eric Howell	SERC
	Robert Melis	California Independent System Operator
	David Gatson	Arizona Public Service (APS)
	Derek Cherneski	Saskatchewan Power Corporation
	Christopher White	Duke Energy
PMOS Liaison	Colby Bellville	Cooperative Energy
NERC Staff	Alison Oswald – Standards Developer	NERC
	Nina Johnston – Legal	NERC
	Marisa Hecht – Legal	NERC

FERC Order 866

- January 23, 2020, the Federal Energy Regulatory Commission (FERC) issued Order No. 866 approving CIP-012-1
- The Order approving CIP-012 also included an additional directive
  - The order directed NERC to develop modifications to the CIP Reliability Standards to require protections regarding the *availability* of communication links and data communicated between bulk electric system Control Centers
  - Order 866 also stated, “maintaining the availability of communication networks and data should include provisions for incident recovery and continuity of operations in a responsible entity's compliance plan.”

Where we are…

- Revised draft language based on comments
  - Removed proposed R2
  - Incorporated *availability* into approved R1 language

- Supplemental Documentation
  - Updated Technical Rationale
  - Updated Implementation Guidance
  - Response to Comments
  - Implementation Plan

Modified Requirement R1

Proposed* R1
CIP-012 revisions

Availability **incorporated into already approved R1 language**

R1. The Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) to mitigate the risks posed by unauthorized disclosure, unauthorized modification, and loss of availability of data used for Real-time Assessment and Real-time monitoring while such data is being transmitted between any applicable Control Centers. The Responsible Entity is not required to include oral communications in its plan. The plan shall include: [Violation Risk Factor: Medium] [Time Horizon: Operations Planning]

* Draft language – Subject to change

Modified Requirement R1

Proposed* R1 Subparts CIP-012-2 revisions

***Availability* incorporated into already approved R1 language**

1.1 Identification of security and availability protection(s) used to mitigate the risks posed by unauthorized disclosure, unauthorized modification and loss of availability of data used for Real-time Assessment and Real-time monitoring while such data is being transmitted between Control Centers;

1.2 Identification of methods to be used for the recovery of communication links used to transmit Real-time Assessment and Real-time monitoring data between Control Centers;

1.3 Identification of where the Responsible Entity applied security and availability protection(s) as required in Part 1.1; and

1.4 If the Control Centers are owned or operated by different Responsible Entities, identification of the responsibilities of each Responsible Entity for applying security and availability protection(s) to the transmission of Real-time Assessment and Real-time monitoring data between those Control Centers.

* Proposed draft language as of 11/08/2021 – Subject to change

Existing R1 Subparts CIP-012-1

1.1. Identification of security protection used to mitigate the risks posed by unauthorized disclosure and unauthorized modification of Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers;

1.2. Identification of where the Responsible Entity applied security protection for transmitting Real-time Assessment and Real-time monitoring data between Control Centers; and

1.3. If the Control Centers are owned or operated by different Responsible Entities, identification of 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.

Proposed* Technical Rationale and Implementation Guidance

What is "Availability"?

- Availability is defined as, "Ensuring timely and reliable access to and use of information" - from: NIST SP 800-59 under "Availability" from 44 U.S.C., Sec. 3542 (b)(1)(C)
- Scoping is important – CIP-012-2 is scoped to further refine the term availability to "timely and reliable transmission of" RTA and RTM data as it is transmitted between applicable Control Centers.
  - RTA and RTM data "at rest" is already protected via other CIP Standards.
  - In here, "timely" is largely defined via the Responsible Entity's implementation of the TOP and IRO Standards.
  - The timeliness (timeframes) and the use of the data is well established in the O&P Standards.

* Proposed as of 11/08/2021 – Subject to change

Proposed* Technical Rationale and Implementation Guidance

R1.1 Identification of Security and Availability Protections

- RTA and RTM data has a quality component (IRO-010 and TOP-003)
- The O&P defined time constraints must be met per the O&P Standards
  - The time constraints are an O&P defined component, not CIP.
  - The availability component of CIP-012 covers the *movement* of RTA and RTM data.
- Availability can be achieved utilizing diversity, redundancy, or a combination of both.
  - Diversity - using heterogeneity to minimize common mode failures.
  - Redundancy - providing multiple protected instances of critical resources.

* Proposed as of 11/08/2021 – Subject to change

Proposed* Technical Rationale and Implementation Guidance

R1.2 Identification of Methods Used for Recovery of Links

- The CIP-012 Plan should identify the information needed to recover data communication links used for transmission of RTA and RTM data.
- May or may not be BES Cyber Assets.
- Other plans (e.g. CIP-009 plans) may be referenced within the CIP-012 plan.
  - If another plan is used but components of the CIP-012 protections fall outside of the scope of the other plan, they should be addressed.
  - May be addressed inside the CIP-012 plan or as part of the other plan.

* Proposed as of 11/08/2021 – Subject to change

Proposed* Technical Rationale and Implementation Guidance

R1.3 Identification of Where Security and Availability Protections are Applied

- "Where" is the "what" addressed? R1.1 is what we do, R1.3 is where we did it.
- Is there a separate discreet circuit? Are there redundant systems? Both?
- The CIP-012 Plan should describe in enough detail the components used to provide protections, as well as where the components reside, to demonstrate adequate coverage.
- Again, protection components may or may not be BES Cyber Assets and may or may not reside within an ESP/PSP.
- When physically outside a PSP, the components must still have physical protections.

* Proposed as of 11/08/2021 – Subject to change

Proposed* Technical Rationale and Implementation Guidance

R1.4 Control Centers "owned or operated by different Responsible Entities"…

- The SDT included subpart R1.4 to address security and availability concerns as well as audit concerns.
- Both entities should understand the responsibilities around applying controls to ensure the in-scope data is protected through its entire transmission and ensure there is no gap in required protections.
- This requirement subpart will provide evidence which may prevent the simultaneous auditing of multiple entities.
- Example evidence may include a joint procedure, a memorandum of understanding, or meeting minutes, documenting the defined responsibilities between the two parties.

* Proposed as of 11/08/2021 – Subject to change

Implementation Plan

24-month implementation plan to allow for (if needed):

- An appropriate technical analysis of existing data transfer capabilities.
- Planning, budgeting and procuring any additional technology needed to meet availability objective.
- Implementing additional technology to facilitate meeting the objectives.
- Testing newly implemented technology to ensure that the objectives are met.
- Ensuring that any desired agreements, *MOUs or contracts with other Registered Entities are drafted, agreed upon and implemented.

* MOU – Memorandum of Understanding

Posting

- Second Draft of CIP-012-2
  - Clean and redline versions
- Implementation Plan
- Updated Technical Rationale for CIP-012
- Updated Implementation Guidance
- Posting Dates
  - 55-Day Additional Comment Period
    - November 30, 2021 – January 24, 2022
  - Ballot Period
    - January 14, 2022 – January 24, 2022
- Project Page

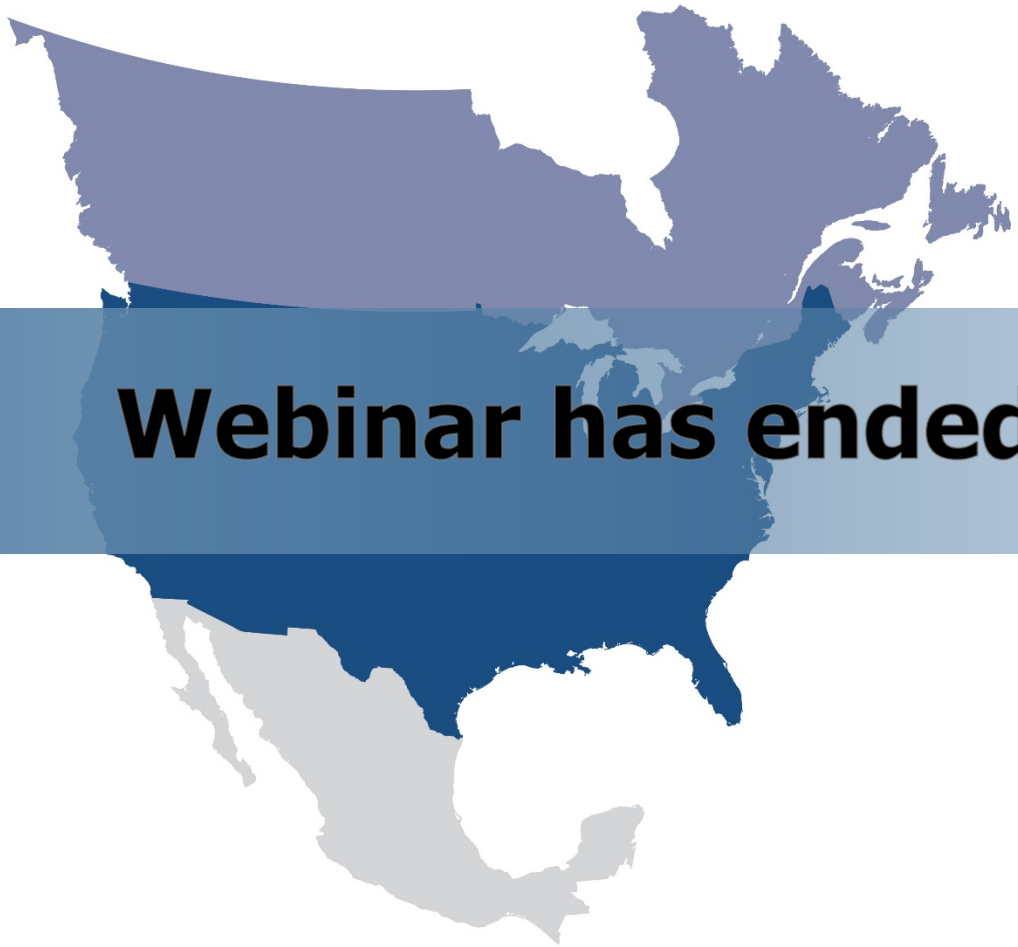
Next Steps

- Respond to Comments
  - Team Meetings starting in February
  - Projected third Posting in April
- Point of Contact
  - Alison Oswald, Senior Standards Developer
  - Alison.oswald@nerc.net or call 404-446-9668
- Webinar Posting
  - 48-72 hours
  - Standards Bulletin

Q & A Objectives

- Informal Discussion
  - Via the Q&A feature
  - Chat only goes to the host, not panelists
  - Respond to stakeholder questions
- Other
  - Some questions may require future team consideration
  - Please reference slide number, standard section, etc., if applicable
  - Team will address as many questions as possible
  - Webinar and chat comments are not a part of the official project record
  - Questions regarding compliance with existing Reliability Standards should be directed to ERO Enterprise compliance staff, not the Standard Drafting Team

Questions and Answers



Webinar has ended – Thank You