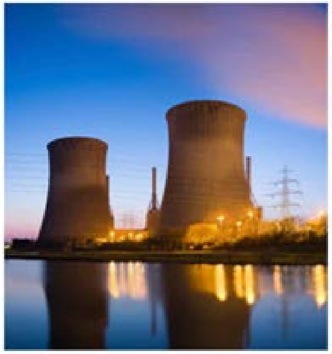
NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Project 2020-04 Update Modifications to CIP-012

October 24, 2022

RELIABILITY | RESILIENCE | SECURITY



Agenda

Administrative

- Review NERC Antitrust Compliance Guidelines and Public Announcement

Agenda

- 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.

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.”

“Comment Themes”

- Split the previously proposed R1.1 into R1.1 and a new R1.2
  - R1.1 to address “Security Protections” while the new R1.2 will address “Availability Controls”.
  - Splitting protections from controls allows the Measures to better reflect how entities can demonstrate compliance.
- Rethink how Measures are incorporated
  - What is a Measure? “A Measure provides identification of the evidence or types of evidence that may demonstrate compliance with the associated requirement.“[1]
  - There were regulatory certainty concerns within the industry.
  - The use of the Measures within the Standard helps guide both entities and auditors toward common evidence.
- Defining “Availability”
  - The concept of availability is integral to the Standard and is represented in the Measures, Implementation Guidance, and Technical Rationale.
  - Using the NIST definitions as a basis allows flexibility in *how* Responsible Entities provide for availability.

[1] Drafting Team Reference Manual, Version 3

Where we are…

- Remember – this is a CIP Standard. *Cyber* remains the focus:
  - CIP-012 implementation should demonstrate ***cyber protections and controls*** (the CIA triad).
- Standard subparts have been modified based on comments.
  - The term "availability" has been removed from the Standard subparts.
  - Split R1.1 into a separate R1.1 and a new R1.2
  - "Identification of method(s)" update and more descriptive Measures for each subpart.
  - Have a plan that identifies your methods. Follow your plan.
- Updated Supplemental Documentation:
  - Updated Technical Rationale, Implementation Guidance and Response to Comments.
- Implementation Plan language remains unchanged (24 months)

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]

Modified Requirement R1

Proposed R1 Subparts CIP-012-2 revisions

R1.1 Identification of method(s) used to mitigate the risks posed by unauthorized disclosure and unauthorized modification of data used for Real-time Assessment and Real-time monitoring while such data is being transmitted between Control Centers;
R1.2 Identification of method(s) used to mitigate the risk(s) posed by loss of data used for Real-time Assessment and Real-time monitoring while such data is being transmitted between Control Centers
R1.3 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;
R1.4 Identification of where the Responsible Entity implemented method(s) as required in Parts 1.1 and 1.2; and
R1.5 If the Control Centers are owned or operated by different Responsible Entities, identification of the responsibilities of each Responsible Entity for implementing method(s) as required in Parts 1.1 and 1.2.

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.

"Methods"

Identification of Methods Language

"Identification of method(s) used to mitigate the risks posed by…"

- Have a plan that identifies your methods. Implement the plan.
- The requirement to "identify methods" allows Registered Entities to implement controls and measures to mitigate risk while quantifying what was done by describing the methods used within the plan.
- Measures for the subparts have been expanded within the Standard language to give a limited number of examples of what *could* be used as part of your plan.
- Remember – Measures are not requirements.
    - *They represent "a way"* or *"several ways…" to produce an evidence stack.*
    - Measures are *"including, but not limited to…"*

“Why 1.2 *and* 1.3”

R1.2 *and* R1.3

R1.2 Identification of method(s) used to mitigate the risk(s) posed by loss of data used for Real-time Assessment and Real-time monitoring while such data is being transmitted between Control Centers;

- What do I do to “protect or account for” availability?
- These represent <u>preventative</u> measures and controls.

R1.3 Identification of method(s) to be used for the *recovery* of communication links used to transmit Real-time Assessment and Real-time monitoring data between Control Centers;

- What do I do if/when an in-scope link goes down?
- These are <u>corrective</u> measures and controls.

A deeper dive into R1.2

Looking at R1.2

R1.2 Mitigate Risk Posed by Loss

R1.2 “Identification of method(s) used to mitigate the risk(s) posed by loss of data used for Real-time Assessment and Real-time monitoring while such data is being transmitted between Control Centers;”

- New subpart to separate availability into its own subpart with a focus on measures or controls rather than protections.
- More consistent with achieving a results-based approach than the previous draft.
- Allows the responsible entities more flexibility in *how* they demonstrate the availability requirement.

R1.3 – Recovery

Order 866 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.”

R1.3 “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; “

- “What do we do to restore the Control Center link if it goes down?”
- Standard operating procedures, CIP-009 recovery plan, or similar technical recovery plans.
- Call the provider? Call the internal helpdesk? Follow SOP-123? Consult the CIP-009 recovery plan?
- Make sure that elements of the Control Center to Control Center communication path that fall outside of the scope of any referenced pre-existing plans or procedures are addressed.

Where?

R1.4 – Where?

R1.4 "Identification of where the Responsible Entity implemented method(s) as required in Parts 1.1 and 1.2"

- Physically where are physical and / or logical protection(s) applied?
- Where are the "methods used to mitigate the risk posed by loss" applied?

Remember: The following are **representative** of ways in which an entity may demonstrate compliance.

- DDOS protection applied by provider at their demarcation point.
- Redundancy provided by "Circuit A and Circuit B" as indicated on this network diagram.
- Physical protections applied at these locations to physically protect the circuit(s).

R1.5 – Control Centers Owned by Different Entities

R1.5 “If the Control Centers are owned or operated by different Responsible Entities, identification of the responsibilities of each Responsible Entity for implementing method(s) as required in Parts 1.1 and 1.2.”

- The change here is the use of methods identified in R1.1 and R1.2 since the previous draft included availability in the “protections” statement.
- “Who is responsible for what when in-scope data is sent and received from another Responsible Entity.”

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

Note: Unchanged from previous draft

Posting

- Third Draft of CIP-012-2
  - Clean and redline versions
- Implementation Plan (remains 24 months)
- Updated Technical Rationale for CIP-012
- Updated Implementation Guidance
- Posting Dates
  - 45-Day Additional Comment Period
    - October 3 – November 16, 2022
  - Ballot Period
    - November 7 – 16, 2022
- Project Page

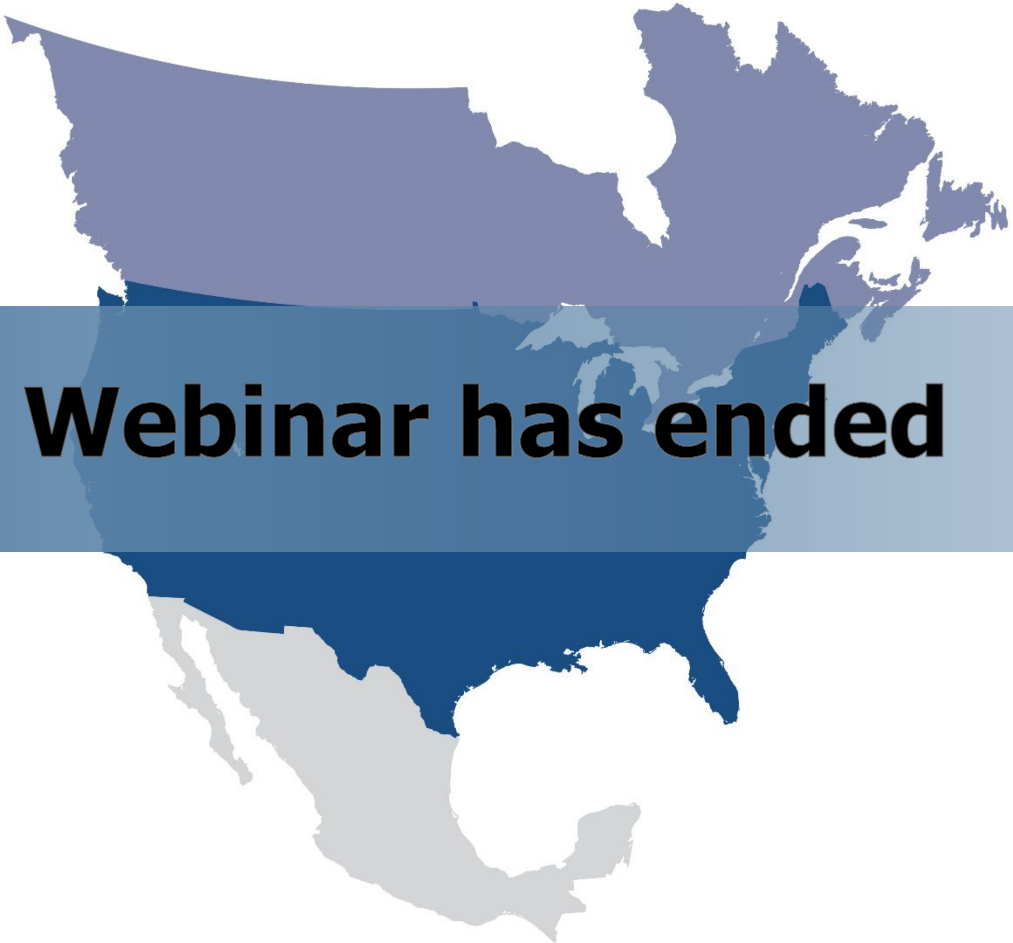
Next Steps

- Response to Comments
  - Team meetings in late November
  - Projected Final Ballot in January 2023
- 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