NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Project 2022-05

Modifications to CIP-008 Reporting Thresholds

Industry Outreach
July 2024

RELIABILITY | RESILIENCE | SECURITY




Administrative Items

- NERC Antitrust Guidelines
  - 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.
- Notice of Open Meeting
  - Participants are reminded that this webinar is public. The access number was widely distributed. Speakers on the call should keep in mind that the listening audience may include members of the press and representatives of various governmental authorities, in addition to the expected participation by industry stakeholders.

Agenda

- Project Overview
- SDT Approach
- Overview of Proposed Revisions
  - Definitions
  - Core Content Changes R1-R4
  - Implementation Plan

Project Overview

- Project Overview
- Security Objective
  - SAR Scope
    - NERC Effectiveness Study
    - FERC CIP Audit Lessons Learned
    - Definitions, CIP-008, CIP-003
  - Priority and Timeline
    - Low priority in Standards Development Project List
    - Earliest first posting for comment and ballot expected in Q4 2024

SDT Approach

- SDT Approach
  - Followed related INSM project (CIP-015-1)
  - Consideration of other existing standards
    - CIP-004-7 R4-R6 – Events detected during access reviews, or revocation processing.
    - CIP-005-7 R1.5 – Detect known or suspected malicious communications.
    - CIP-006-6 R1 Part 1.5 – alarms/alerts of unauthorized access to a PSP
    - CIP-007-6 R3.2 – Mitigate the threat of detected malicious code.
    - CIP-007-6 R4.1 – Review log events.
    - CIP-007-6 R4.2 – Alerts for logging failures or detected malware.
    - CIP-007-6 R4.4 – Log review to identify undetected Cyber Security Incidents.
    - CIP-007-6 R5.7 – Threshold exceeded alerts; unsuccessful authentication attempts.
    - CIP-009-6 R1 Part 1.4 – Detected backup failures
    - CIP-010-4 R1 / R2.1 – Deviations from existing baseline.
    - CIP-011-R1-R2 – Insecure handling or unauthorized disclosure of BCSI.
    - CIP-012-1 R1 – Failure of security protection of RTA/RTm in transit.
    - CIP-013-2 R1.2 – Notification of vendor breaches or incidents
  - Brief update on formatting

Overview of Proposed Revisions

- Overview of Proposed Revisions
  - Definitions
  - Core Content Changes:
    - R1
    - R2
    - R3
    - R4
  - Implementation Plan

Overview of Proposed Revisions

- Approach
  - Starting with NIST definitions (realignment)
  - Removal of “requirement” language from definitions
  - Removal of scoping language from definitions
- Proposed Definition Changes
  - Modified Definition – Cyber Security Incident
  - New Definitions:
    - Event of Interest
    - Attempted Cyber Security Incident
  - Retire Definition - Reportable Cyber Security Incident

Cyber Security Incident

- **Cyber Security Incident (current)**

  A malicious act or suspicious event that:

  - For a high or medium impact BES Cyber System, compromises or attempts to compromise

  (1) an Electronic Security Perimeter, (2) a Physical Security Perimeter, or (3) an Electronic Access Control or Monitoring System; or

  - Disrupts or attempts to disrupt the operation of a BES Cyber System

- **NIST Cybersecurity Incident –**

  A cybersecurity event that has been determined to have an impact on the organization prompting the need for response and recovery.

- **Cyber Security Incident (Proposed)**

  An Event of Interest that has had an impact on the organization's cyber security prompting the need for response.

NEW

Event of Interest

- **Event of Interest** –

  Detected anomalous or suspicious activity that may have an impact on the organization's cyber security prompting the need for investigation.

- Aligns closely with NIST Glossary terms
  - **"relevant event,"**
    - An occurrence (e.g., an auditable event or flag) considered to have potential security implications to the system or its environment that may require further action (noting, investigating, or reacting).
  - **"cybersecurity event"**
    - "A cybersecurity change that may have an impact on organizational operations (including mission, capabilities, or reputation)."

Attempted Cyber Security Incident

NEW

- **Attempted Cyber Security Incident –**

  An Event of Interest that may have an impact on the organization's cyber security prompting the need for response.

Reportable Cyber Security Incident

- **Reportable Cyber Security Incident (Retire)**

  A Cyber Security Incident that compromised or disrupted:

  - A BES Cyber System that performs one or more reliability tasks of a functional entity;
  - An Electronic Security Perimeter of a high or medium impact BES Cyber System; or
  - An Electronic Access Control or Monitoring System of a high or medium impact BES Cyber System

Requirement R1

Core Content Changes – Requirement R1

R1. Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include each of the applicable requirement parts in *CIP-008-6 Table R1 – Cyber Security Incident Response Plan Specifications*. *[Violation Risk Factor: Lower] [Time Horizon: Long Term Planning].*

CIP-008-6 Table R1 – Cyber Security Incident Response Plan Specifications

Part	Requirements
1.1	One or more processes to identify, classify, and respond to Cyber Security Incidents.
1.2	One or more processes: 1.2.1 That include criteria to evaluate and define attempts to compromise; 1.2.2 To determine if an identified Cyber Security Incident is: • A Reportable Cyber Security Incident; or • An attempt to compromise, as determined by applying the criteria from Part 1.2.1, one or more systems identified in the "Applicable Systems" column for this Part; and 1.2.3 To provide notification per Requirement R4.
1.3	The roles and responsibilities of Cyber Security Incident response groups or individuals.
1.4	Incident handling procedures for Cyber Security Incidents.

R1. Each Responsible Entity shall document one or more cyber security plan(s), for high and medium impact BCS and their associated EACMS, that collectively include: *[Violation Risk Factor: Lower] [Time Horizon: Long Term Planning].*

1.1 Intake process for Events of Interest NEW

1.2 Response to Events of Interest that meet the definition of either Attempted Cyber Security Incident or Cyber Security Incident;

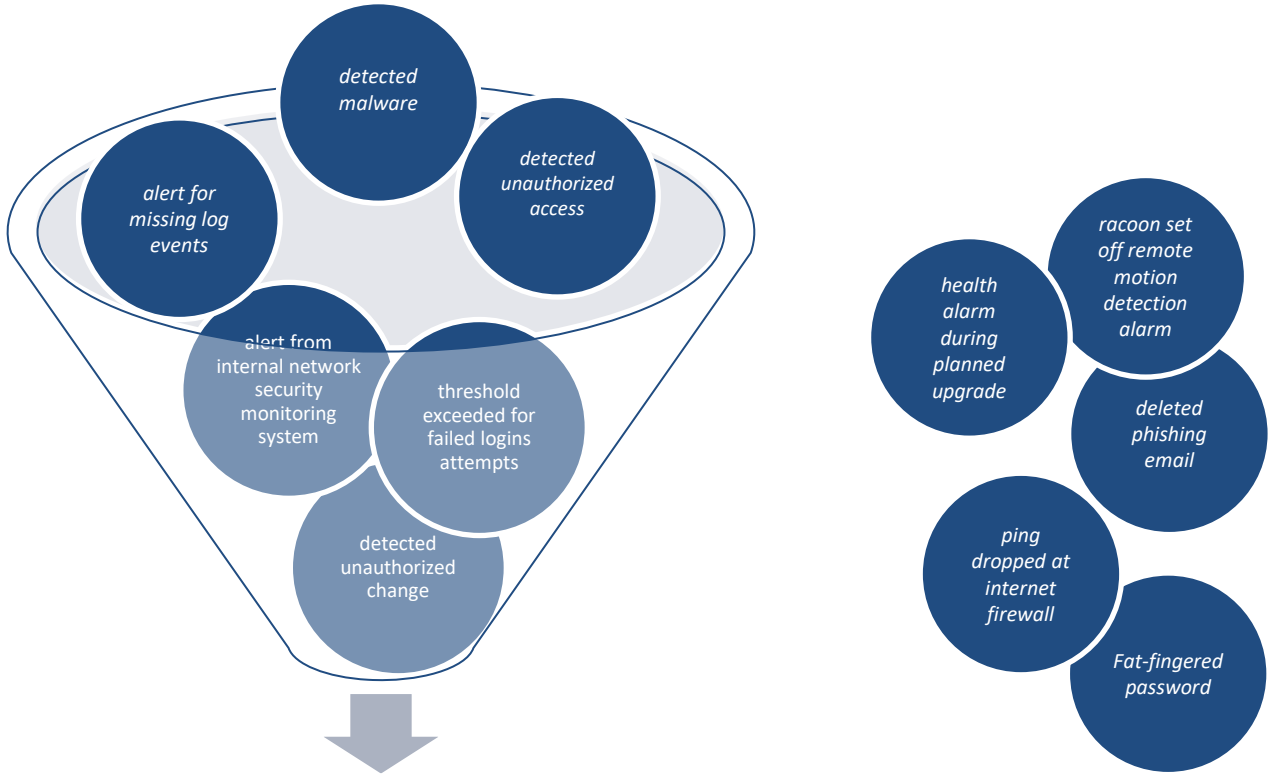
1.3 Roles and responsibilities of response groups or individuals;

1.4 Incident handling procedures for either Attempted Cyber Security Incidents or Cyber Security Incidents; and

1.5 Notification per Requirement R4.

Requirement R1

- Core Content Changes – Requirement Part 1.1



Requirement R1 Part 1.2 – 1.4

- Core Content Changes – Requirement R1 Part 1.2 – 1.4

R1. Each Responsible Entity shall maintain each of its Cyber Security Incident response plans according to each of the applicable requirement parts in *CIP-008-6 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

CIP-008-6 Table R1 – Cyber Security Incident Response Plan Specifications	
Part	**Requirements**
1.1	One or more processes to identify, classify, and respond to Cyber Security Incidents.
1.2	One or more processes: 1.2.1. That include criteria to evaluate and define attempts to compromise; 1.2.2. To determine if an identified Cyber Security Incident is: • A Reportable Cyber Security Incident; or • An attempt to compromise, as determined by applying the criteria from Part 1.2.1, one or more systems identified in the "Applicable Systems" column for this Part; and 1.2.3. To provide notification per Requirement R4.
1.3	The roles and responsibilities of Cyber Security Incident response groups or individuals.
1.4	Incident handling procedures for Cyber Security Incidents

R1. Each Responsible Entity shall document one or more cyber security plan(s), for high and medium impact BCS and their associated EACMS, that collectively include: *[Violation Risk Factor: Lower] [Time Horizon: Long Term Planning].*

1.1. Intake process for Events of Interest;

1.2. Response to Events of Interest that meet the definition of either Attempted Cyber Security Incident or Cyber Security Incident;

1.3. Roles and responsibilities of response groups or individuals;

1.4. Incident handling procedures for either Attempted Cyber Security Incidents or Cyber Security Incidents; and

1.5. Notification per Requirement R4.

Requirement R2

- Core Content Changes – Requirement R2
  - Summary of changes
    - Impact of shift to cyber security plans
    - Reversing 2.1 and 2.2
    - Scope 2.2 testing to current enforceable

Requirement R2

- Core Content Changes in R2

R2. Each Responsible Entity shall implement each of its documented Cyber Security Incident response plans to collectively include each of the applicable requirement parts in *CIP-008-6 Table R2 – Cyber Security Incident Response Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-Time Operations].*

CIP-008-6 Table R2 – Cyber Security Incident Response Plan Implementation and Testing

Part	Requirements
2.1	Test each Cyber Security Incident response plan(s) at least once every 15 calendar months: • By responding to an actual Reportable Cyber Security Incident; • With a paper drill or tabletop exercise of a Reportable Cyber Security Incident; or • With an operational exercise of a Reportable Cyber Security Incident.
2.2	Use the Cyber Security Incident response plan(s) under Requirement R1 when responding to a Reportable Cyber Security Incident, responding to a Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for this Part, or performing an exercise of a Reportable Cyber Security Incident. Document deviations from the plan(s) taken during the response to the incident or exercise.
2.3	Retain records related to Reportable Cyber Security Incidents and Cyber Security Incidents that attempted to compromise a system identified in the "Applicable Systems" column for this Part as per the Cyber Security Incident response plan(s) under Requirement R1.

R2. Each Responsible Entity shall implement each of its documented cyber security plans for Requirement R1 to collectively include: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-Time Operations].*

2.1. Using the cyber security plan(s) under Requirement R1 when responding to Events of Interest that meet the definition of either Attempted Cyber Security Incident or Cyber Security Incident.

2.2. Testing of Requirement R1 Part 1.2 through 1.5 of each cyber security plan(s) at least once every 15 calendar months:

- By responding per Part 2.1;
- With a paper drill or tabletop exercise; or
- With an operational exercise.

2.3. Documentation of deviations from the plan(s) taken during the response to the incident or exercise.

2.4. Retention of records related to Events of Interest that meet the definition of either Attempted Cyber Security Incident or Cyber Security Incident as per the cyber security plan(s) under Requirement R1.

Requirement R3

- Core Content changes in R3.1 only

R3. Each Responsible Entity shall maintain each of its Cyber Security Incident response plans according to each of the applicable requirement parts in *CIP-008-6 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

CIP-008-6 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication

Part	Requirements
3.1	No later than 90 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response: 3.1.1. Document any lessons learned or document the absence of any lessons learned; 3.1.2. Update the Cyber Security Incident response plan based on any documented lessons learned associated with the plan; and Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates to the Cyber Security Incident response plan based on any documented lessons learned. 3.1.3. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates to the Cyber Security Incident response plan based on any documented lessons learned.

R3. Each Responsible Entity shall maintain each of its cyber security plan(s) for Requirement R1 according to each of the following timeframes: *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

3.1 No later than 90 calendar days after a completion of a test or actual use of a cyber security plan(s):

- 3.1.1 Review deviations from the plan documented in Requirement R2.3; NEW
- 3.1.2 Document any incident response lessons learned that require changes to the plan or document the absence of any lessons learned;
- 3.1.3 Update the cyber security plan(s); and
- 3.1.4 Notify response groups or individuals with a defined role in the cyber security plan(s) of the updates.

Requirement R4

- Core Content changes in R4 and Part 4.2 only

R4. Each Responsible Entity shall notify the Electricity Information Sharing and Analysis Center (E-ISAC) and, if subject to the jurisdiction of the United States, the United States National Cybersecurity and Communications Integration Center (NCCIC),[1] or their successors, of a Reportable Cyber Security Incident and a Cyber Security Incident that was an attempt to compromise, as determined by applying the criteria from Requirement R1, Part 1.2.1, a system identified in the "Applicable Systems" column, unless prohibited by law, in accordance with each of the applicable requirement parts in *CIP-008-6 Table R4 – Notifications and Reporting for Cyber Security Incidents*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

CIP-008-6 Table R4 – Notifications and Reporting for Cyber Security Incidents

Part	Requirements
4.2	After the Responsible Entity's determination made pursuant to documented process(es) in Requirement R1, Part 1.2, provide initial notification within the following timelines: • One hour after the determination of a Reportable Cyber Security Incident. • By the end of the next calendar day after determination that a Cyber Security Incident was an attempt to compromise a system identified in the "Applicable Systems" column for this Part.

R4. Each Responsible Entity shall notify the Electricity Information Sharing and Analysis Center (E-ISAC) and, if subject to the jurisdiction of the United States, the United States Cybersecurity and Infrastructure Security Agency (CISA), or their successors, of Events of Interest that meet the definition of either Attempted Cyber Security Incident or Cyber Security Incident unless prohibited by law, in accordance with the following reporting specifications and timeframes *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

4.2. After the Responsible Entity's determination made pursuant to documented process(es) in Requirement R1, provide initial notification within the following timelines:

4.2.1. One hour after the determination of a Cyber Security Incident affecting high or medium impact BCS or their associated EACMS.

4.2.2. By the end of the next calendar day after determination of an Attempted Cyber Security Incident affecting high or medium impact BCS or their associated EACMS.

CIP-003 Conforming Changes

Mirror changes from CIP-008 in CIP-003

Includes streamlining to cyber security plan(s), in both R2 and Attachment 1 then:

1. **Intake process** (mirrors CIP-008 R1 Part 1.1)
2. **Respond to incident** (mirrors CIP-008 R1 Part 1.2)
3. **Define roles & responsibilities** (mirrors CIP-008 R1 Part 1.3)
4. **Incident handling procedures** (mirrors CIP-008 R1 Part 1.4)
5. **Notification** (mirrors CIP-008 R1 Part 1.5)
6. **Testing** (mirrors CIP-008 R2)
7. **Plan updates** (Mirrors CIP-008 R3)

CIP-003 Conforming Changes

Section 4. Cyber Security Incident Response: Each Responsible Entity shall have one or more cyber security plan(s) for low impact BES Cyber Systems, either by asset or group of assets, which shall include:

4.1 Intake process for Events of Interest;

4.2 Response to Events of Interest that meet the definition of Cyber Security Incident;

4.3 Roles and responsibilities of response groups or individuals;

4.4 Incident handling procedures for Cyber Security Incidents;

4.5 Notification to the Electricity Information Sharing and Analysis Center (E-ISAC) and, if subject to the jurisdiction of the United States, the United States Cybersecurity and Infrastructure Security Agency (CISA), or their successors, of Events of Interest that meet the definition of Cyber Security Incident, unless prohibited by law;

4.6 Testing the cyber security plan(s) at least once every 36 calendar months by: (1) responding to an actual Cyber Security Incident; (2) using a drill or tabletop exercise of a Cyber Security Incident; or (3) using an operational exercise of a Cyber Security Incident; and

4.7 Updating the cyber security plan(s), if needed, within 180 calendar days after completion of a cyber security plan(s) test or actual Cyber Security Incident.

Implementation Plan

- Implementation Plan
  - Looking at 12-month plan
  - Need to determine specifics for periodic requirements

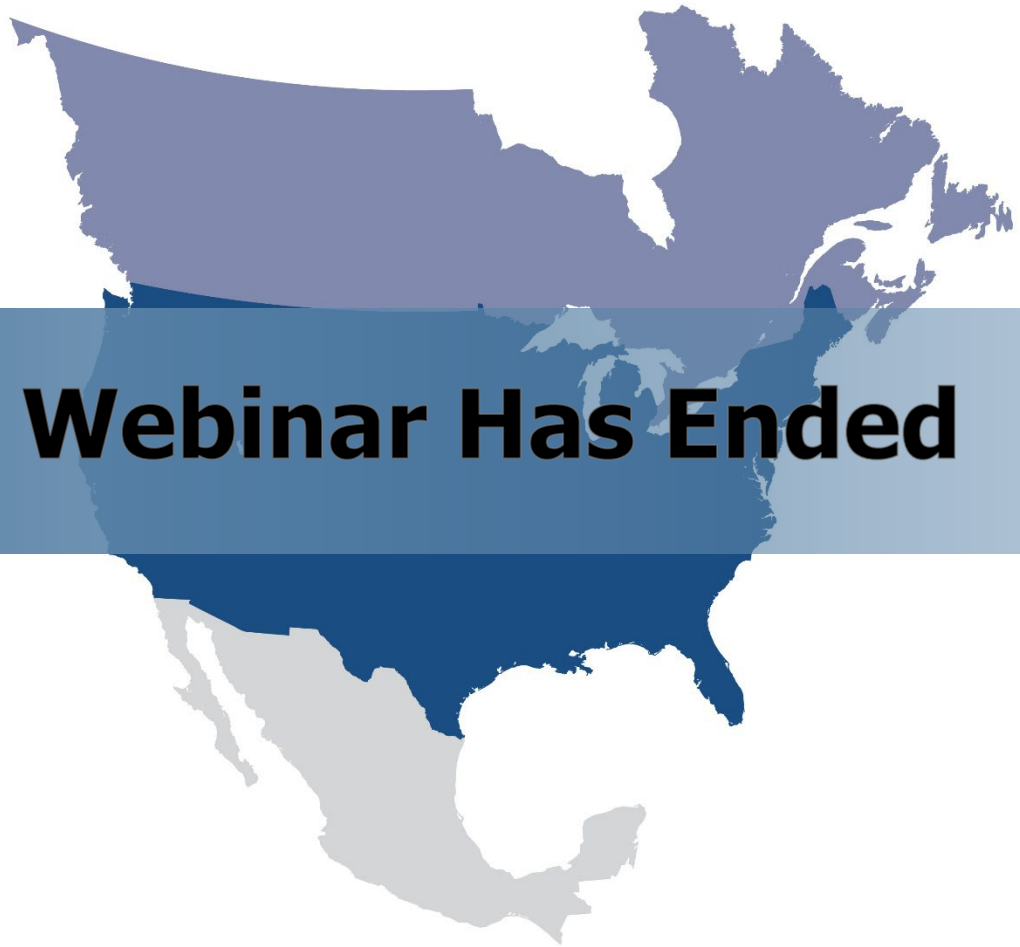
Drafting Team

Name		Company	Email address
Tony	Hall	LG&E and KU Energy	tony.hall@lge-ku.com
Sharon	Koller	American Transmission Company, LLC	skoller@atcllc.com
Marc	Child	Great River Energy	mchild@GREnergy.com
Lawrence	Good	Bonneville Power Administration	lmgood@bpa.gov
Brent	Howell	Duke Energy	brent.howell2@duke-energy.com
Scott	Klauminzer	Tacoma Public Utilities	sklauminzer@cityoftacoma.org
Joshua	Rowe	WECC	JRowe@wecc.org
Bryan	Yoch	Ameren	byoch@ameren.com
Alison	Oswald	NERC	alison.oswald@nerc.net
Jason	Snider	NERC	jason.snider@nerc.net

Questions and Answers Objectives

- Informal Discussion
  - Via the Questions and Answers Objectives feature
  - Chat only goes to the host, not panelists
  - Respond to stakeholder questions
- Other
  - 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 SDT

Questions and Answers



Webinar Has Ended