NERC

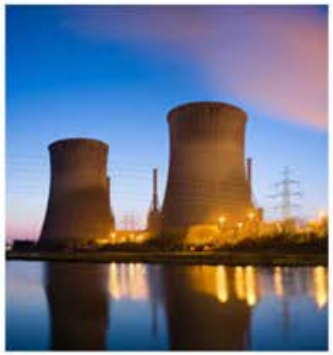
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Industry Webinar

Project 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting

October 16, 2018

RELIABILITY | ACCOUNTABILITY

Agenda

- Presenters
  - Standard Drafting Team

Chair, Dave Rosenthal, MISO	Vice Chair, Kristine Martz, Exelon
Member, Sharon Koller, ATC	Member, Tony Hall, LG&E

  - NERC Staff - Alison Oswald
- Administrative Items
- Project 2018-02 Status
- FERC Order No. 848
- Proposed Definitions
- Requirement Language
- Reporting Form
- 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

- Public Announcement
  - 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.
- Presentation Material
  - Information used herein is used for presentation purposes and may not reflect the actual work of the official posted materials
- For the official record
  - This presentation is not a part of the official project record
  - Comments must be submitted during the formal posting

Status of Project 2018-02

- This is the formal initial posting
  - 20-day comment period
  - 5-day ballot period (October 18-22)
- CIP-008-6 addresses:
  - FERC Order 848

Chair Remarks

>> BALANCE <<

Standard Drafting Team (SDT)

Name	Organization/ Company
David Rosenthal (Chair)	Midcontinent Independent System Operator (MISO)
Kristine Martz (Vice Chair)	Exelon Corporation
Katherine Anagnost	Minnkota Power
Steve Brain	Dominion Energy
John Breckenridge	Kansas City Power & Light Company
Norm Dang	Independent Electricity System Operator
John Gasstrom	Georgia System Operations Corporation
Tony Hall	Louisville Gas & Electric Kentucky Utilities
Ian King	Xcel Energy
Sharon Koller	American Transmission Company, LLC
Jennifer Korenblatt	PJM Interconnection, LLC
Tina Weyand	EDP Renewables

FERC Order 848 Details – Slide 1 of 2

FERC Order 848	
Order Issue Date: July 19, 2018	Order Publish Date: July 31, 2018
Order Effective Date: October 1, 2018	Directive Filing Deadline: April 1, 2019

- Augment reporting to include Cyber Security Incidents that compromise or attempt to compromise a Responsible Entity's Electronic Security Perimeter or associated Electronic Access Control or Monitoring Systems

- Required information in Cyber Security Incident reports should include certain minimum information to improve the quality of reporting and allow for ease of comparison by ensuring that each report includes specified fields of information

FERC Order 848 Details – Slide 2 of 2

FERC Order 848	
Order Issue Date: July 19, 2018	Order Publish Date: July 31, 2018
Order Effective Date: October 1, 2018	Directive Filing Deadline: April 1, 2019

- Filing deadlines for Cyber Security Incident reports should be established once a compromise or disruption to reliable BES operation, or an attempted compromise or disruption, is identified by a Responsible Entity

- Reports should continue to be sent to the E-ISAC, but the reports should also be sent to the Department of Homeland Security (DHS) Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)

Definition / Glossary of Terms Updates

New Terms in the NERC Glossary of Terms:

- Proposed **Modified** Definitions (2):
  - Cyber Security Incident
  - Reportable Cyber Security Incident
- Proposed **New** Definition:
  - Reportable Attempted Cyber Security Incident
- Proposed **Retirements** of Approved Definitions:
  - Cyber Security Incident
  - Reportable Cyber Security Incident

Definition / Glossary of Terms Updates

New Terms in the NERC Glossary of Terms:

Proposed <u>Modified</u> Definition (1 of 2):

- **Cyber Security Incident:**
  - A malicious act or suspicious event that:
    - Compromises, or was an attempt to compromise, (1) the Electronic Security Perimeter, (2) or Physical Security Perimeter, or (3) Electronic Access Control or Monitoring System for High or Medium Impact BES Cyber Systems, or
    - Disrupts, or was an attempt to disrupt, the operation of a BES Cyber System.

Definition / Glossary of Terms Updates

New Terms in the NERC Glossary of Terms:

Proposed <u>Modified</u> Definition (2 of 2):

- **Reportable Cyber Security Incident:**
  - A Cyber Security Incident that has compromised or disrupted:
    - One or more reliability tasks of a functional entity; or
    - Electronic Security Perimeter; or
    - Electronic Access Control or Monitoring System (EACMS) that provide any of the following functions: (1) authentication; (2) monitoring and logging; (3) access control; (4) Interactive Remote Access; or (5) alerting

Definition / Glossary of Terms Updates

New Terms in the NERC Glossary of Terms:

Proposed New Definition:

- **Reportable Attempted Cyber Security Incident:**
  - A Cyber Security Incident that was an attempt to compromise or disrupt:
    - One or more reliability tasks of a functional entity; or
    - Electronic Security Perimeter; or
    - Electronic Access Control or Monitoring System (EACMS) that provide any of the following functions: (1) authentication; (2) monitoring and logging; (3) access control; (4) Interactive Remote Access; or (5) alerting

Definition / Glossary of Terms Updates

New Terms in the NERC Glossary of Terms:

Proposed Retirement of Approved Definitions (2):

- **Cyber Security Incident:**
  - A malicious act or suspicious event that:
    - Compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter or,
    - Disrupts, or was an attempt to disrupt, the operation of a BES Cyber system.
- **Reportable Cyber Security Incident:**
  - A Cyber Security Incident that has compromised or disrupted one or more reliability tasks of a functional entity.

Requirement Language

- R1 – Cyber Security Incident Response Plan Specifications

  - Part 1.1 – 1.4
    - Added EACMS to the Applicable Systems under both High and Medium Impact BES Cyber Systems

  - Part 1.2
    - Moved all notification language to the new Requirement R4

Requirement Language

- R2 – Cyber Security Incident Response Plan Implementation and Testing

- R3 – Cyber Security Incident Response Plan Review, Update, and Communication

  - Part 2.1 – 2.3 and Part 3.1 - 3.2
    - Added EACMS to the Applicable Systems under both High and Medium Impact BES Cyber Systems

Requirement Language

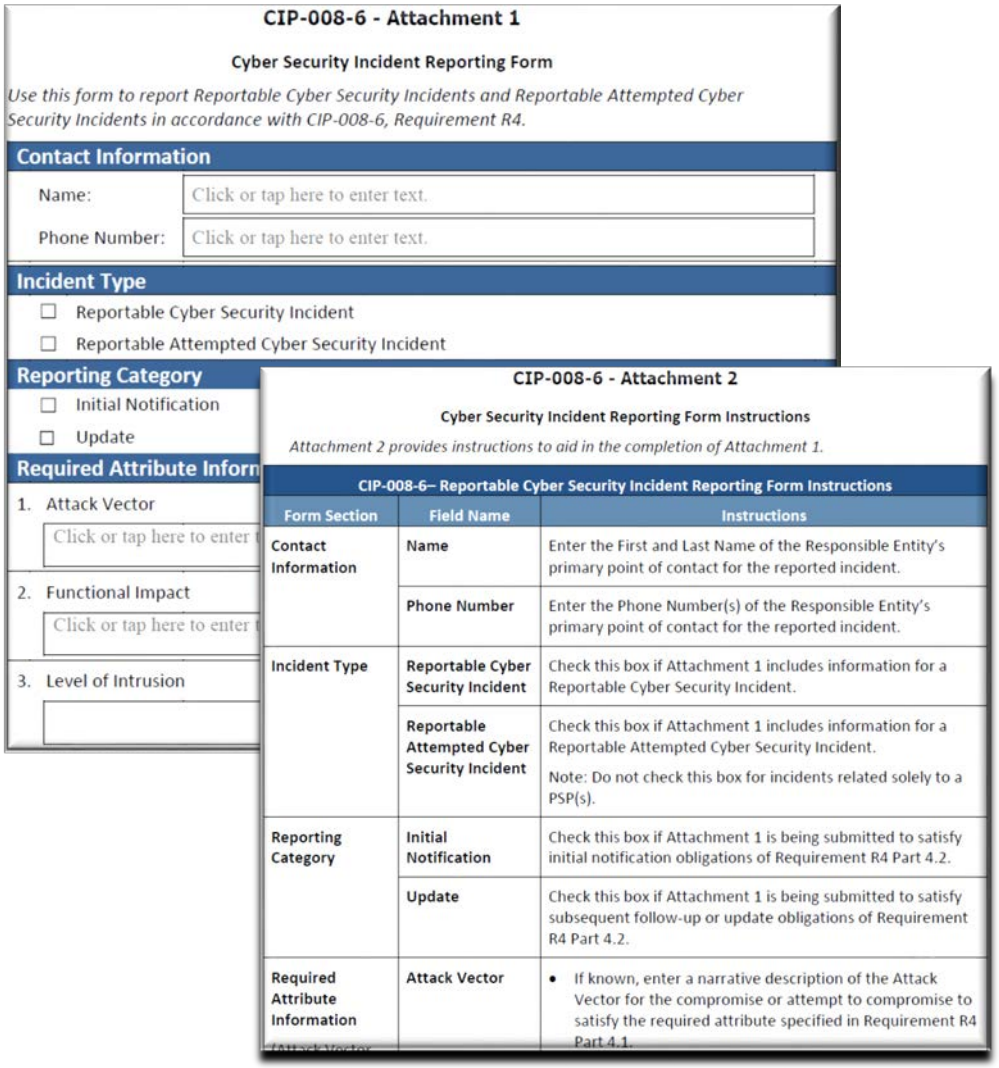
- R4 – Notifications and Reporting for Cyber Security Incidents
  - Part 4.1 – 4.2
    - Added EACMS to the Applicable Systems under both High and Medium Impact BES Cyber Systems
    - Part 4.1
      - Details the attributes that must be included in the reporting: functional impact; attack vector; and level of intrusion
    - Part 4.2
      - Details the methods for initial notification to both E-ISAC and ICS-CERT

Requirement Language

- R4 – Notifications and Reporting for Cyber Security Incidents
  - Part 4.3 – 4.4
    - Added EACMS to the Applicable Systems under both High and Medium Impact BES Cyber Systems
    - Part 4.3
      - Details the timing for initial notification
    - Part 4.4
      - Details the requirement for reporting updates and/or changes to the required attributes

Attachment 1

- Our Biggest Challenge
- "What" versus "How"
  - Why we chose to include
- Content Approach
  - Review Rationale
- Attachment
  - Achieves alignment
  - Provides consistency
  - Available at launch



CIP-008-6 - Attachment 1

Cyber Security Incident Reporting Form

Use this form to report Reportable Cyber Security Incidents and Reportable Attempted Cyber Security Incidents in accordance with CIP-008-6, Requirement R4.

Contact Information

Name: Click or tap here to enter text.

Phone Number: Click or tap here to enter text.

Incident Type

☐ Reportable Cyber Security Incident

☐ Reportable Attempted Cyber Security Incident

Reporting Category

☐ Initial Notification

☐ Update

Required Attribute Inform

1. Attack Vector

Click or tap here to enter

2. Functional Impact

Click or tap here to enter

3. Level of Intrusion

CIP-008-6 - Attachment 2

Cyber Security Incident Reporting Form Instructions

Attachment 2 provides instructions to aid in the completion of Attachment 1.

CIP-008-6– Reportable Cyber Security Incident Reporting Form Instructions

Form Section	Field Name	Instructions
Contact Information	Name	Enter the First and Last Name of the Responsible Entity's primary point of contact for the reported incident.
	Phone Number	Enter the Phone Number(s) of the Responsible Entity's primary point of contact for the reported incident.
Incident Type	Reportable Cyber Security Incident	Check this box if Attachment 1 includes information for a Reportable Cyber Security Incident.
	Reportable Attempted Cyber Security Incident	Check this box if Attachment 1 includes information for a Reportable Attempted Cyber Security Incident. Note: Do not check this box for incidents related solely to a PSP(s).
Reporting Category	Initial Notification	Check this box if Attachment 1 is being submitted to satisfy initial notification obligations of Requirement R4 Part 4.2.
	Update	Check this box if Attachment 1 is being submitted to satisfy subsequent follow-up or update obligations of Requirement R4 Part 4.2.
Required Attribute Information	Attack Vector	• If known, enter a narrative description of the Attack Vector for the compromise or attempt to compromise to satisfy the required attribute specified in Requirement R4 Part 4.1.

Next Steps

- Comment period
  - Project 2018-02 page
  - 20-Day Comment – October 3 – 22, 2018
  - 5-Day Ballot – October 18 - 22, 2018
- Respond to Comments
  - November 2018
- Point of contact
  - Alison Oswald, Senior Standards Developer
  - Alison.oswald@nerc.net or call 404-446-9669
- 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 and Answers

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Webinar has ended – Thank You