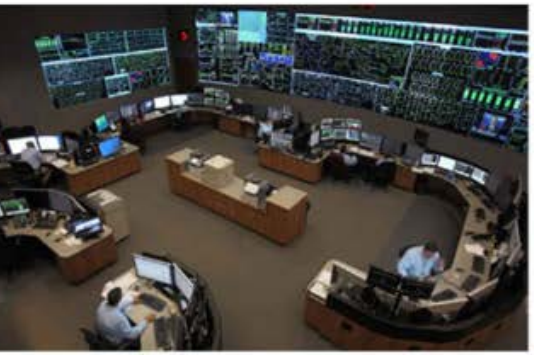
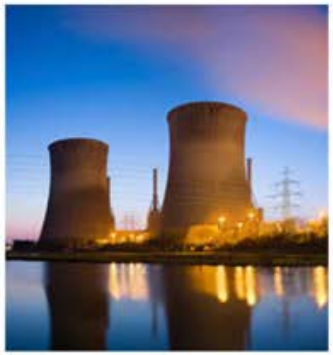
NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

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

RELIABILITY | RESILIENCE | SECURITY

Agenda

- FERC Order 848
- Modified Definitions
- Applicable Systems
- Requirements
- Acknowledgements

FERC Order 848 Details

- Four Directives:
  - 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
  - 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)

Effective Date

- Approved by FERC on June 20, 2019
- Standard Effective on January 1, 2021

Definition / Glossary of Terms Updates

Terms in the NERC Glossary of Terms:

- **Modified** Definitions (2):
  - Cyber Security Incident
  - Reportable Cyber Security Incident
- **Retirements** of previously Approved Definitions that exist in the NERC Glossary with effective dates of 7/1/2016:
  - Cyber Security Incident
  - Reportable Cyber Security Incident

Definition / Glossary of Terms Updates

Modified Definition (1 of 2):

- **Cyber Security Incident:**
  - 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

Definition / Glossary of Terms Updates

Modified Definition (2 of 2):

- **Reportable Cyber Security Incident:**
  - A Cyber Security Incident that has 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

Applicable Systems

- **All requirements have updated applicable systems from:**
  - Applicable to High and Medium Impact BES Cyber Systems
- To:
  - Applicable to High Impact BES Cyber Systems and their associated EACMS and Medium Impact BES Cyber Systems and their associated EACMS

Changes to Requirement: R1

Requirement	CIP-008-5	CIP-008-6
1.1	One or more processes to identify, classify, and respond to Cyber Security Incidents.	No Change beyond Applicable Systems
1.2	One or more processes to determine if an identified Cyber Security Incident is a Reportable Cyber Security Incident and notify the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), unless prohibited by law. Initial notification to the ES-ISAC, which may be only a preliminary notice, shall not exceed one hour from the determination of a Reportable Cyber Security Incident.	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.	No Change beyond Applicable Systems
1.4	Incident handling procedures for Cyber Security Incidents.	No Change beyond Applicable Systems

Changes to Requirement: R2

Requirement	CIP-008-5	CIP-008-6
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.	No Change beyond Applicable Systems
2.2	Use the Cyber Security Incident response plan(s) under Requirement R1 when responding to a Reportable Cyber Security Incident 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.	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.

Changes to Requirement: R2

Requirement	CIP-008-5	CIP-008-6
2.3	Retain records related to Reportable Cyber Security Incidents.	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.

Changes to Requirement: R3

Requirement	CIP-008-5	CIP-008-6
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 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.	No Change beyond Applicable Systems
3.2	No later than 60 calendar days after a change to the roles or responsibilities, Cyber Security Incident response groups or individuals, or technology that the Responsible Entity determines would impact the ability to execute the plan: 3.2.1. Update the Cyber Security Incident response plan(s); and 3.2.2. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates.	No Change beyond Applicable Systems

Changes to Requirement: R4

Requirement	CIP-008-5	CIP-008-6
4.1	Does not Exist	Initial notifications and updates shall include the following attributes, at a minimum, to the extent known: 4.1.1 The functional impact; 4.1.2 The attack vector used; and 4.1.3 The level of intrusion that was achieved or attempted.
4.2	Does not Exist	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.
4.3	Does not Exist	Provide updates, if any, within 7 calendar days of determination of new or changed attribute information required in Part 4.1.

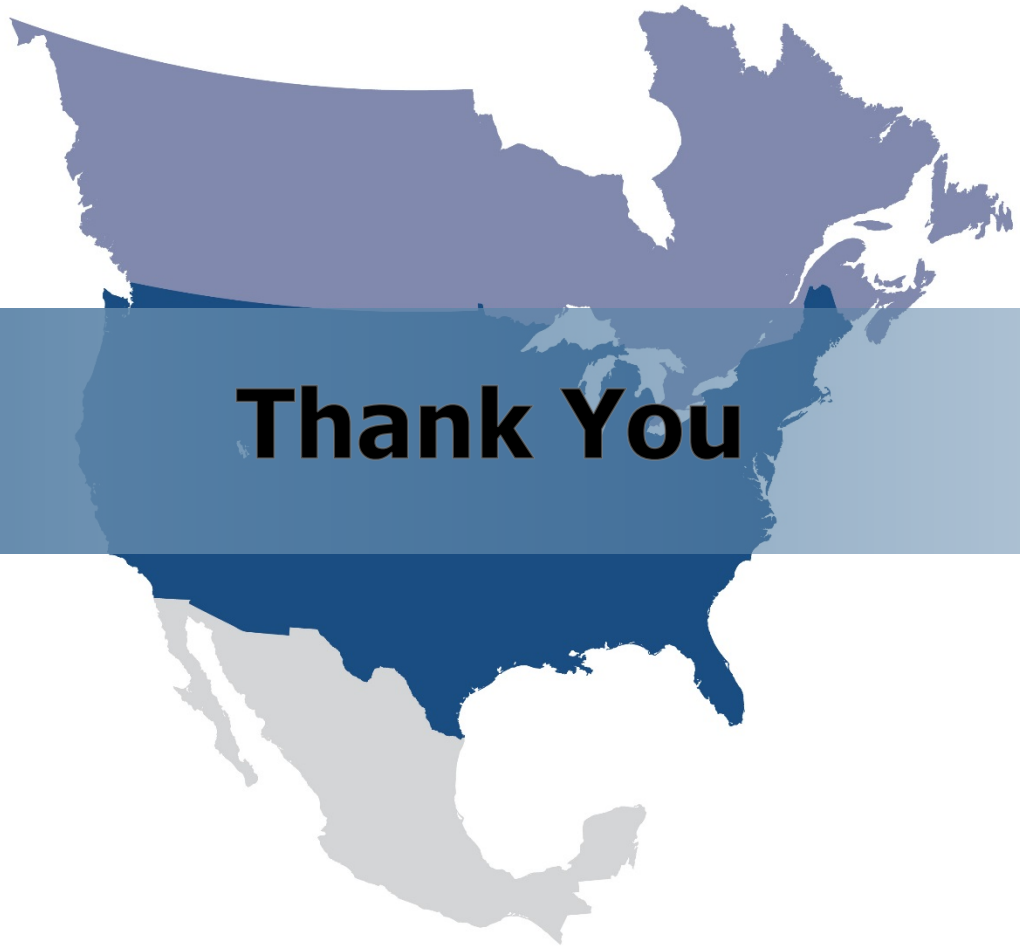
Implementation Guidance

- Draft Implementation Guidance is currently going through ERO approval
  - Found on the project page

Acknowledgements

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
Marisa Hecht	NERC, Counsel
Alison Oswald	NERC, Senior Standards Developer

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION



Thank You