

# Implementation Plan

## Project 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting | Reliability Standard CIP-008-6

### Applicable Standard and Definitions

- CIP-008-6 – Cyber Security – Incident Reporting and Response Planning
- Glossary of Terms Used in NERC Reliability Standards Definition of Cyber Security Incident
- Glossary of Terms Used in NERC Reliability Standards Definition of Reportable Cyber Security Incident

### Requested Retirements

- CIP-008-5 – Cyber Security – Incident Reporting and Response Planning
- Glossary of Terms Used in NERC Reliability Standards Definition of Cyber Security Incident (currently effective definition)
- Glossary of Terms Used in NERC Reliability Standards Definition of Reportable Cyber Security Incident (currently effective definition)

### Prerequisite Standard(s)

These standard(s) or definitions must be approved before the Applicable Standard becomes effective: None

### Applicable Entities

- Balancing Authority
- Distribution Provider
- Generator Operator
- Generator Owner
- Reliability Coordinator
- Transmission Operator
- Transmission Owner

### ~~New Terms in the NERC Glossary of Terms~~

~~This section includes all newly defined, revised, or retired terms used or eliminated in the NERC Reliability Standard. New or revised definitions listed below become approved when the proposed~~

~~standard is approved. When the standard becomes effective, these defined terms will be removed from the individual standard and added to the *Glossary of Terms Used in NERC Reliability Standards*.~~

**~~Proposed Modified Definitions:~~**

~~Cyber Security Incident:~~

~~A malicious act or suspicious event that:~~

- ~~• For a high or medium impact BES Cyber System, cCompromises, or was an attempt to compromise the, (1) an Electronic Security Perimeter, (2) a Physical Security Perimeter, or (3) an Electronic Access Control or Monitoring Systems for High or Medium Impact BES Cyber Systems; 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:~~

- ~~• A BES Cyber System that performs one or more reliability tasks of a functional entity;~~
- ~~• Electronic Security Perimeter(s); or~~
- ~~• Electronic Access Control or Monitoring Systems.~~

**~~Proposed Retirements of Approved Definitions:~~**

~~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.~~

**Background**

The purpose of this project is to address the directives that FERC issued i-by FERC in Order No. 848 to augment mandatory reporting of Cyber Security Incidents, including attempted Cyber Security Incidents that might facilitate subsequent efforts to harm the Reliable Operation of the Bulk Electric System (BES). FERC directed NERC to develop and submit modifications that would “require the reporting of Cyber Security Incidents that compromise, or attempt to compromise, a responsible entity’s Electronic Security Perimeter (ESP) or associated Electronic Access Control or Monitoring Systems (EACMS).” (Order No. 848 at P1)

Proposed Reliability Standard CIP-008-6 addresses the four<sup>4</sup> elements outlined by FERC:

1. Responsible entities must report Cyber Security Incidents that compromise, or attempt to compromise, a responsible entity’s ESP or associated EACMS;

2. 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;
3. Establish deadlines for filing Cyber Security Incidents that are commensurate with incident severity; and
4. Cyber Security Incident reports should be sent to the Electricity Information Sharing and Analysis Center (E-ISAC) and [the United States National Cybersecurity and Communications Integration Center \(NCCIC\)](#),<sup>1</sup>~~the Department of Homeland Security (DHS) Industrial Control Systems Cyber Emergency Response Team (ICS-CERT).~~

## Effective Date

### Reliability Standard CIP-008-6

Where approval by an applicable governmental authority is required, the standard shall become effective on the first day of the first calendar quarter that is 18 calendar months after the effective date of the applicable governmental authority's order approving the standard, or as otherwise provided for by the applicable governmental authority.

Where approval by an applicable governmental authority is not required, the standard shall become effective on the first day of the first calendar quarter that is 18 calendar months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

### Revised Definitions for Cyber Security Incident and Reportable Cyber Security Incident

Where approval by an applicable governmental authority is required, the definition shall become effective on the first day of the first calendar quarter that is 18 calendar months after the effective date of the applicable governmental authority's order approving Reliability Standard CIP-008-6, or as otherwise provided for by the applicable governmental authority.

Where approval by an applicable governmental authority is not required, the definition shall become effective on the first day of the first calendar quarter that is 18 calendar months after the date that Reliability Standard CIP-008-6 is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

## Retirement Date

### Reliability Standard CIP-008-5

---

<sup>1</sup> [The National Cybersecurity and Communications Integration Center \(NCCIC\) is the successor organization of the Industrial Control Systems Cyber Emergency Response Team \(ICS-CERT\). In 2017, NCCIC realigned its organizational structure and integrated like functions previously performed independently by the ICS-CERT and the United States Computer Emergency Readiness Team \(US-CERT\).](#)

Reliability Standard CIP-008-5 shall be retired immediately prior to the effective date of Reliability Standard CIP-008-6 in the particular jurisdiction in which the revised standard is becoming effective.

**Currently Effective Definitions for Cyber Security Incident and Reportable Cyber Security Incident**

The definitions proposed for retirement shall be retired immediately prior to the effective date of Reliability Standard CIP-008-6 in the particular jurisdiction in which the revised standard is becoming effective.