NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DRAFT

Cyber Security – Incident Report

Technical Rationale and Justification for Reliability Standard CIP-008-6

October 2018

RELIABILITY | ACCOUNTABILITY



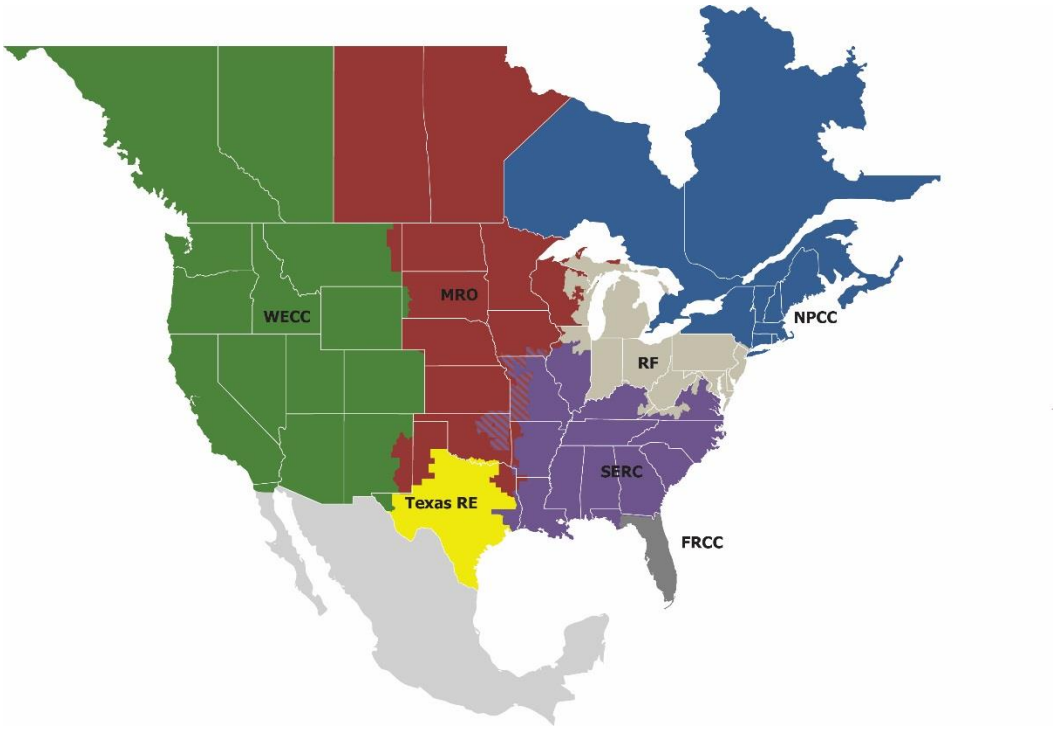

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Preface

The vision for the Electric Reliability Organization (ERO) Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the seven Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

The North American BPS is divided into seven RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.



FRCC	Florida Reliability Coordinating Council
MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-008-6. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. It also contains information on the Standard Drafting Team's (SDT's) intent in drafting the requirements. This Technical Rationale and Justification for CIP-008-6 is not a Reliability Standard and should not be considered mandatory and enforceable.

On July 19, 2018, the Federal Energy Regulatory Commission (FERC or Commission) issued Order No. 848, where the FERC directed the North American Electric Reliability Corporation (NERC) to "develop and submit modifications to the Reliability Standards to 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 and Control or Monitoring System (EACMS)." (Order 848, Paragraph 1)

In response to the directive in Order No. 848, the Project 2018-02 SDT drafted Reliability Standard CIP-008-6 to require Responsible Entities to implement methods augmenting the mandatory reporting of Cyber Security Incidents to include: "(1) responsible entities must report Cyber Security incidents that compromise, or attempt to compromise, a responsible entity's ESP; (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 included specified fields of information; (3) 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; and (4) Cyber Security Incident reports should continue to be sent to the Electricity Information Sharing and Analysis Center (E-ISAC), rather than the Commission, but the reports should also be sent to the Department of Homeland Security (DHS) Industrial Control System Cyber Emergency Response Team (ICS-CERT)." (Order 848, Paragraph 3)

New and Modified Terms Used in NERC Reliability Standards

Proposed Modified Terms:

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.*

The SDT modified the Cyber Security Incident definition to add part (3), above, to include Electronic Access Control or Monitoring Systems (EACMS) in response to the Order. FERC Order 848, Paragraph 1, directs the modification of the Reliability Standards to require the reporting of Cyber Security Incidents to include the responsible entity's ESP(s) (already included above) or associated EACMS (which the SDT added to the above definition).

The SDT considered potential unintended consequences related to the use of the existing definition in CIP-003-6 and qualified the addition of Electronic Access Control or Monitoring Systems with '*High or Medium Impact BES Cyber Systems'* to assure clarity and the SDT's intentions to exclude low impact.

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*

The SDT also modified the Reportable Cyber Security Incident definition to comply with FERC Order 848. The SDT modified the Reportable Cyber Security Incident definition to include incidents that compromised or disrupted an ESP or an EACMS that provides specific functions, as directed by the Order. (Order 848, Paragraph 54)

The SDT considered potential unintended consequences related to the use of the existing definition in CIP-003-6 and qualified the addition of Electronic Access Control or Monitoring Systems with '*High or Medium Impact BES Cyber Systems'* to assure clarity and the SDT's intentions to exclude low impact.

Proposed New Term:

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*

The SDT created this new definition to clarify attempted Cyber Security Incidents subject to reporting. FERC Order 848 specifically directs modifying the Reliability Standard(s) to require reporting of attempted compromises for ESP(s) or associated EACMS(s). The SDT included the list of EACMS functions to clarify the parameters of Reportable Attempted Cyber Security Incidents related to EACMS.

The Order specifically required the reporting of attempts to compromise for ESP, and EACMS, the SDT included "One or more reliability tasks of a functional entity in the definition to be consistent with Reportable Cyber Security Incidents.

Requirements R1, R2, and R3

General Considerations for Requirement R1, Requirement R2, and Requirement R3

FERC Order 848, Paragraph 1, which directs modifications to Reliability Standards to require reporting of incidents that compromise, or attempt to compromise a responsible entity's ESP or associated EACMS. The intent of the SDT was to minimize the changes within CIP-008 while also addressing the required changes, thus the SDT added "and their associated EACMS" to the "Applicable Systems" column for Requirements R1, R2, and R3.

Moving Parts of Requirement R1 to Requirement R4

To minimize the changes to Requirement R1 the SDT created Requirement R4 and consolidated all the CIP-008-6 reporting requirements. The SDT deleted the Requirement R1 Part 1.2 reporting requirements and moved them to Requirement R4 to serve this purpose.

Inclusion of "Successor Organizations" throughout the Requirement Parts

The SDT recognizes that organizations are constantly evolving to meet emerging needs, and may re-organize or change their names over time. The ICS-CERT has recently begun to change its name to the National Cybersecurity and Communications Integration Center (NCCIC) Industrial Control Systems, and the E-ISAC has previously re-branded their name and may again in the future. By following Requirement R4 references to E-ISAC and ICS-CERT with "or their successors" the SDT intended to ensure Requirement R4 can be implemented even if the names of E-ISAC and ICS-CERT change or a different agency take over their current role.

Reported Attempted Cyber Security Incidents not eligible to meeting testing requirement

Requirement R2 Part 2.1 requires a test of the responsible entity's incident response plan for a Reportable Cyber Security Incident. The SDT debated whether testing incident response plans for a Reportable Attempted Cyber Security Incident would also meet the Requirement R2 Part 2.1 testing requirement. However, the SDT concluded that testing only the parts of a responsible entity's incident response plan required to respond to an attempt to compromise applicable Cyber Systems would not subject the testing to the same rigor as a response to an actual compromise.

Requirement R4

General Considerations for Requirement R4

Requirement R4 is a new requirement focused on mandatory reporting of Reportable Cyber Security Incidents and newly-defined Reportable Attempted Cyber Security Incidents (refer to Proposed New Term, above). Previously, CIP-008-5 defined reporting requirements for Reportable Cyber Security Requirements (Requirement R1 Part 1.2) only.

Required Reportable Incident Attributes

Requirement R4.1 specifies that initial notifications and updates include three attributes: 1) functional impact, 2) attack vector used, and 3) level of intrusion achieved or attempted. These attributes are taken directly from the Order. (FERC Order No. 848, paragraph 89).

The SDT understands that some or all of these attributes may be unknown at time of initial notification, thus added "to the extent known" to account for this scenario.

Methods for Submitting Notifications

Requirement R4 Part 4.2 specifies responsible entities shall use one of three methods for initial notification. The SDT endeavored to provide latitude in reporting methods and format for initial notification, to allow responsible entities' personnel to focus on incident response itself and not methods and format of reporting in this stage of incident response. The SDT defined three initial notification methods to provide a measure of standardization industry-wide. While Requirement R4 Part 4.2 allows for several methods of initial notification, it also requires submission of Attachment 1 to facilitate standardized reporting.

- *Electronic submission of Attachment 1* – The SDT envisions this as a simple email with Attachment 1 attached. However, the requirement is written to be broad enough that should either E-ISAC or ICS-CERT, or their successors, offer other options for submitting Attachment 1 like a web portal, this would still be within the requirement language.
- *Phone* – The SDT sees notification via telephone as a reasonable format for initial notification as it is quick and allows personnel to get back to incident response expeditiously.
- *Email* – In this context, a manually populated or automatically generated email can be submitted by simply including the required attributes without any specific format directly in an email to E-ISAC and ICS-CERT, or their successors. Again, the SDT views this as a quicker reporting method that could be used as a preliminary method to notify during incident response.

The last paragraph of the requirement was included to ensure that known data in a common format is eventually submitted via Attachment 1, as a common form allows for easier summarization, correlation, and trending of events.

Notification Timing

Requirement R4 Part 4.3 specifies two timelines for notification submission: one hour for Reportable Cyber Security Incidents and end of next calendar day for Reportable Attempted Cyber Security Incidents. FERC Order No 848 directly states that reporting deadlines must be established in paragraph 3, and later in paragraph 89 states that "timelines that are commensurate with the adverse impact to the BES that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES."

- *Reportable Cyber Security Incidents* – The SDT wrote Part R4.3 to use a one hour deadline for reporting of these events, as incidents in this category include successful penetrations of ESPs, EACMS or BES Cyber Systems. One hour is referenced directly in FERC Order No 848 paragraph 89 and is also the current reporting requirement in CIP-008-5.

Requirement R4

- *Reportable Attempted Cyber Security Incidents* – Due to the lower severity of these unsuccessful attempts at penetrating ESP(s), EACMS, or BES Cyber Systems, the SDT proposed a longer reporting timeframe. The intent behind the decision to add "By the end of the next calendar day (11:59 pm local time)" was to afford responsible entities additional time to gather facts prior to notifications for the less severe Reportable Attempted Cyber Security Incident category.
- *Initial* submission may be by made by one of the three methods described above. The SDT understands that initial notification may not have all the details, but when Attachment 1 or an email is submitted, it is expected that information that has been determined is reported within the notification deadlines.

Notification Updates

Requirement R4 Part 4.4 requires that responsible entities shall submit Attachment 1 updates for the required attributes upon determination of new or changed attribute information. The SDT added this language to provide responsible entities sufficient time to determine attribute information, which may be unknown at the time of initial notification and which may change as more information is gathered. The intent of Requirement R4 Part 4.4 is to provide a method for responsible entities to report new information over time as investigations progress. NOTE: The SDT does not intend Attachment 1 updates specified in Requirement R4. Part 4.4 to expose responsible entities to potential violations if, for instance, an initial notification on an attribute and an updated notification on the same attribute have different information, since knowledge of attributes may change as investigations proceed. Rather, the intent of Requirement R4 Part 4.4 is to have a mechanism to report incident information to E-ISAC and ICS-CERT, or their successors, (and therefore, industry) upon determination of each required attribute.

Attachment 1

General Considerations for Attachment 1

As discussed above in Requirement R4 rationale, the SDT created Attachment 1 to provide a standard method for reporting to both E-ISAC and ICS-CERT or their successors until a time comes where an online portal may be developed. Since the Order directs requiring reporting to both agencies, a standard format will allow responsible entities to complete a single form and submit it to both agencies. (Order 848, Paragraph 3)

There was debate among the SDT on what to include in Attachment 1, and the SDT decided to include only those elements required by FERC Order 848, to assure required attributes are captured and minimize risk of possible violations for the responsible entities submitting the form. The SDT discussed potentially proposing modifications to DOE Form OE-417 to meet the directives in the Order, however, with the recent updates of OE-417 by DOE and timing of the Order, the SDT determined there was not enough time to make those modifications. The SDT interpreted that FERC did not support the use of OE-417, since the Order notes the differences of DOE's definition of a "Cyber Event" and NERC's definition of a Cyber Security Incident. (Order 848, Paragraph 73) Additionally, the SDT had concerns that OE-417 was designed for a different purpose and considered the use of this form for CIP-008 reporting to be inefficient for reporting only the required attributes.

The SDT was purposeful in the design of Attachment 1 to be concise and require limited data. The intent was to ease the burden on responsible entities by providing a method to quickly report required data while protecting entities from concerns with over-reporting and potentially exposing protected information under CIP-004 and CIP-011.