NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

# Consideration of Comments

## Project 2022-05 Modifications to CIP-008 Reporting Threshold

## Comments Received Summary

There were 37 sets of responses, including comments from approximately 96 different people from approximately 72 companies representing 10 of the Industry Segments.

All comments submitted can be reviewed in their original format on the project page.

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process. If you feel there has been an error or omission, you can contact the Vice President of Engineering and Standards, Soo Jin Kim (via email) or at (404) 446-9742.

### Consideration of Comments

The Project 2022-05 Modifications to CIP-008 Reporting Threshold SAR Drafting Team (DT) thanks all of industry for your time and comments. The SAR DT revised the SAR based on industry comments and conversations with FERC and compliance staff. Due to the similar nature of multiple comments received during the SAR comment period, the SAR DT has chosen to respond to comments in summary format as provided for by section 4.2 of the Standard Processes Manual.

**Multiple industry comments were received that do not support the SAR and do not believe any modifications to any CIP Standards are needed nor warranted. Specifically, many comments raised concerns with multiple reports being required.**

The SAR DT acknowledges industry comments and concerns about multiple reporting methods, and the associated administrative burden, and confusion surrounding these challenges. The SAR DT agrees there is opportunity to address this through modifications to the Standards and/or new/modified Definitions. For the SAR DT to consider solutions to this concern, the SAR requires approval.

**Many comments received asked for more information to understand the basis for the SAR and need for this change.**

The SAR DT acknowledges industry comments and concerns about needing additional information to understand the basis for the SAR and the need for change. The SAR DT sought additional data points from FERC and NERC staff and was provided cases and anonymized examples demonstrating a lack of alignment between industry and the ERO on what constitutes an attempt to compromise and when reporting obligations exist[1]. For example, as the standard allows entities to define attempts themselves, some have defined attempts to compromise that would never require reporting separate from Reportable Cyber Security Incident reporting. Failure to communicate Cyber Security Incidents can hinder the electric industry's ability to share security information such as how to help others avoid mistakes made in the detection and response process, mitigate complex malware, understand evolving threats, and identify coordinated cyberattacks to the grid. The SAR DT agrees the current language does not provide the level

[1] Attachment 1

of clarity necessary to assure the intent of the requirement is met. The SAR DT believes there is opportunity to address this through modifications to the Standards and/or new/modified Definitions. For the SAR DT to consider solutions to this concern, the SAR requires approval.

**Comments were received expressing concern that the creation of new, or changes to existing definitions, could have broader ranging impact and unintended scoping consequences with CIP-003 R2.**

The SAR DT acknowledges industry comments and concerns regarding the potential for unintended consequences regarding low impact. The SAR DT agrees a mindful approach must be taken to assure proposed modifications meet the SAR directives and scope. For the SAR DT to consider solutions to this concern, the SAR requires approval.

**Multiple industry comments requested the team leverage existing controls in the suite of Standards to define minimum reporting thresholds for attempts to compromise.**

The SAR DT acknowledges industry comments and the suggestion to consider leveraging existing controls prescribed within the current enforceable suite of the Standards, such as CIP-007 R4 as an example. The SAR DT agrees this may serve as a potential approach to meet the SAR directives, and to gain the clarity and alignment needed between industry and our regulators. The SAR DT agrees there is an opportunity to address this through modifications to the Standards and/or new/modified Definitions. The SAR DT has made modifications to the SAR to provide this flexibility. For the SAR DT to consider this option as a solution, the SAR requires approval.

# Attachment 1

## FERC Staff Audit Observations and NERC CIP-008 Effectiveness Study Observations

The Standard Drafting Team was informed by several examples that reflect a wide disparity in entity interpretation of the existing requirement.

**The following nine examples are of entity criteria to evaluate and define attempts to compromise.**

**Example 1**

Scanning covered cyber systems/assets for vulnerabilities or to verify their existence that is not approved by management nor process(es) (this could be due to an upstream compromise or malware), attempts to access covered cyber systems/assets locally or remotely that fail due to not being authorized and intending to gain access electronically or physically where no approval has been given, or attempts to escalate privileges on covered cyber systems/assets by an authorized user that have been determined to fail due to not being authorized for that privilege level.

**Example 2**

- Detected unauthorized port scanning of the Electronic Security Perimeter (ESP) (not involving other company infrastructure);
- An attempt to deliberately install malware using a physical on-site vector;
- Use of credentials that can be proven to be sourced from someone that is an unauthorized source;
- Alert from security monitoring systems on Applicable Systems that is proven to be from an unauthorized person (e.g. not from an authorized user or administrator);
- Receipt of a victim notification from FBI or other law enforcement sources related to Applicable Systems; or
- Internal incident is supported by correlating event using <name of security tool>.

**Example 3**

Entity Thresholds: Regular Cyber Events- These are normal cyber events that require no further investigations, such as:

- Scheduled port scans;
- Equipment scanning a Cyber Asset for vulnerabilities or to verify its existence that is performed expected on demand or on an approved periodic schedule; or
- Malicious code simulation exercises.

Low-risk Cyber Events- These are cyber events that could become potential Cyber Security Incidents as they are beyond normal background events and require some level of investigation, but do not require reporting under CIP-008-6, such as:

- Incidents blocked at an Electronic Access Point (EAP) and found not to be malicious or suspicious;
- Attempts to access a Cyber Asset by an authorized user that have been determined to fail due to human error;
- Unexpected successful login outside scheduled working hours; or
- Failed access attempts from unexpected network IP address.

Medium-risk incidents- These are cyber events that are malicious or suspicious and require mitigation activities, but do not require reporting under CIP-008-6, such as:

- Unauthorized Removable Media found in Electronic Access Control or Monitoring Systems (EACMS) or BES Cyber System;
- Responsible personnel owned corporate assets infected with malware attempting to affect other corporate assets, but not targeting a CIP-008-6 applicable asset; or
- Attempts to access a Cyber Asset by a user that fails due to not being authorized and intending to gain access where no approval has been given (non-CIP-008-6 asset).

High-risk incidents- These are cyber events responsible personnel determines were malicious or suspicious and required mitigation activities, and will be reported under CIP-008-6, such as:

- Attempts to access a Cyber Asset by a user that fails due to not being authorized and intending to gain access where no approval has been given (CIP-008-6 asset);
- Responsible personnel owned corporate cyber assets that has been compromised, attempting to affect a CIP-008-6 applicable asset;
- Persistent intrusion attempts detected at the EAP by malicious actor; or
- Removable media with malicious code found connected to an applicable asset.

## Example 4

Entity Thresholds:
Emergency - A cyber incident that investigation found was a Cyber Security Incident that has compromised or disrupted a BCS that performs one or more reliability tasks of a functional entity. Incidents that result in imminent threat to public safety and BES reliability.

Severe - A cyber incident that investigation found was a Cyber Security Incident involving a compromise or disruption of an ESP or EACMS; or a cyber incident that investigation found was a Cyber Security Incident that attempted to compromise BCS Incidents that have the potential to result in a threat to public safety and BES reliability if they continue or escalate. Immediate mitigation is required.

High - A cyber incident that investigation found was an attempt to compromise or disrupt an EACMS or ESP. An attempt to compromise an Applicable System or EACMS. Does not result in a threat to public safety, but still requires mitigation.

Medium - A cyber incident that investigation found was malicious or suspicious, but was not a Cyber Security Incident because it did not target an Applicable System or perimeter. A cyber incident that is malicious or suspicious and required mitigation, but did not target Applicable Systems or EACMS.

Low - A cyber incident that investigation found was not malicious or suspicious. A new network scanning tool creates blocked traffic at the firewall.

Baseline - Inconsequential cyber events: Events that require no investigation and are not cyber incidents. These represent “background noise”. E.g. low- interest, blocked, traffic at the firewall.

**Example 5**

A single event identified by the Security Information and Event Management based on the alerting thresholds that is confirmed to be an attempt to compromise would be classified as a reportable attempt to compromise.

**Example 6**

Entity has established specific triggers and thresholds which require additional scrutiny (event vs. incident) and to establish criteria for what will be reported to the Service Desk or Entity C InfoSec. To enable required external reporting within mandated timeframes, it is important for the Cyber Security Incident Response Team Lead or designee to perform internal notifications as described in internal policy XX.

**Example 7**

An act with malicious intent to gain access or to cause harm to normal operation of a High Impact or Medium Impact BCS or associated EACMS. Accumulated knowledge and professional expertise is relied upon to make the call.

**Example 8**

A cyber security or physical security event that attempts to identify, gain unauthorized access to or influence the operations of a BES Cyber System, Electronic Access Control or Monitoring System, Protected Cyber Asset, Physical Access Control System, Electronic Security Perimeter, Electronic Access Point or Physical Security Perimeter with suspicious or malicious intent, but does not result in unauthorized access or influence the operations of the aforementioned systems.

**Example 9**

a. Attempt must have been detected or prevented by a BES asset, or their associated EACMS, Physical Access Control Systems (PACS) or Protected Cyber Asset (PCA).

b. Intent must have been judged (by the Cybersecurity Director or delegate) to be malicious.

**The following two examples are audit observations.**

**Example 10**

Audit observations include definition of Cyber Security Incident lacks clear criteria of what constitutes a "malicious act" or "suspicious event." Specifically, staff noted some audited entities failed to identify certain events, including verified malware, as being malicious, and therefore did not report, because the incident did not meet the entity's definition of a malicious event. Additionally, an entity had adequate response procedures, however, the entity did not properly activate its plan due to inadequate criteria for identifying malicious acts or suspicious events. As a result, the entity did not follow through and report multiple events.

**Example 11**

Audit observations include definition of Cyber Security Incident lacks clarity of the terms "compromise" and "attempt to compromise." Multiple entities failed to identify certain events, including the presence of verified malware identified on a BES cyber system, as being compromised, and therefore did not report the Cyber Security Incidents. To justify not reporting these compromises, entities provided unreasonable interpretations of the standard. For example, in one instance an entity discovered identified malware on a BES Cyber System, yet determined it was not compromised because the BES Cyber System was isolated and was unable to communicate to the command-and-control server that the malware was beaconing out too. In another instance, an entity found malicious code on an installer, but the installer was in the BES Cyber System's recycle bin and required human interaction to activate the malware, and therefore determined the system was not compromised. In this instance, the entity was focused on the location of the malware and not the fact that unauthorized code was on a system with the potential to perform malicious actions. Additionally, this code may be an indicator of a broader issue for the BES which makes communicating the incident important.