NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DRAFT Implementation Guidance Pending Submittal for ERO Enterprise Endorsement

DRAFT

Cyber Security – Incident Reporting and Response Planning

Implementation Guidance for CIP-008-6

RELIABILITY | ACCOUNTABILITY




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

Table of Contents

List of Figures

Introduction

The Standards Project 2018-02 – Modifications to CIP-008 Standard Drafting Team (SDT) prepared this Implementation Guidance to provide example approaches for compliance with the modifications to CIP-008-6. Implementation Guidance does not prescribe the only approach, but highlights one or more approaches that would be effective in achieving compliance with the standard. Because Implementation Guidance only provides examples, entities may choose alternative approaches that better fit their individual situations.[1]

Responsible entities may find it useful to consider this Implementation Guidance document along with the additional context and background provided in the SDT-developed Technical Rationale and Justification for the modifications to CIP- 008-6.

The Federal Energy Regulatory Commission (the Commission) issued Order No. 848 on July 19, 2018, calling for modifications to the NERC Reliability Standards to augment the mandatory reporting of Cyber Security Incidents, including incidents that might facilitate subsequent efforts to harm the reliable operation of the BES.[2] The Commission 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 Control or Monitoring Systems (EACMS).[3]

The Commission's directive consisted of four elements intended to augment the current Cyber Security Incident reporting requirement: (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) 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 Systems Cyber Emergency Response Team (ICS-CERT) now known as NCCIC[4]. Further, NERC must file an annual, public, and anonymized summary of the reports with the Commission.

The minimum attributes to be reported should include: (1) the functional impact, where possible to determine, that the Cyber Security Incident achieved or attempted to achieve; (2) the attack vector that was used to achieve or attempted to achieve the Cyber Security Incident; and (3) the level of intrusion that was achieved or attempted as a result of the Cyber Security Incident.

The Project 2018-02 SDT drafted Reliability Standard CIP-008-6 to require responsible entities to meet the directives set forth in the Commission's Order No. 848.

---

[1] NERC's Compliance Guidance Policy

[2] 16 U.S.C. 824o(d)(5). The NERC Glossary of Terms Used in NERC Reliability Standards (June 12, 2018) (NERC Glossary) defines a Cyber Security Incident as "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."

[3] The NERC Glossary defines "ESP" as "[t]he logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol." The NERC Glossary defines "EACMS" as "Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Systems."

[4] The DHS ICS-CERT underwent a reorganization and rebranding effort and is now known as the National Cybersecurity and Communications Integration Center (NCCIC).

Definitions

CIP-008-6 has two related definitions, as well as language for "attempts to compromise" that is specific to CIP-008-6 within Requirement R1 Part 1.2.2. Cyber Security Incidents are not reportable until the Responsible Entity determines one rises to the level of a Reportable Cyber Security Incident or meets the Responsible Entity's established criteria pursuant to Requirement R1 Part 1.2.1 and 1.2.2. When these thresholds are reached reporting to both E-ISAC and NCCIC (Formerly DHS's ICS-CERT) is required. These definitions and requirement language are cited below for reference when reading the implementation guidance that follows.

Cyber Security Incident:
A malicious act or suspicious event that:

- Compromises, or was an attempt to compromise the (1) Electronic Security Perimeter, (2) Physical Security Perimeter, (3) 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.

CIP-008-6 Table R1 – Cyber Security Incident Response Plan Specifications		
Part	**Applicable Systems**	**Requirements**
1.2	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	One or more processes to: 1.2.1 Establish criteria to evaluate and define attempts to compromise; 1.2.2 Determine if an identified Cyber Security Incident is: • A Reportable Cyber Security Incident, or • Only an attempt to compromise one or more systems identified in the "Applicable Systems" column for this Part; and 1.2.3 Provide notification per Requirement R4.

The determination of reportability for compromises or disruptions (by definition), or for attempts to compromise (pursuant to the requirement language), becomes a function of applying criteria that builds upon the parent definition of Cyber Security Incident.

The below Venn diagram illustrates the relationships between the elements of each definition, and the Requirement R1 Part 1.2.2 requirement language. In this example, one potential option could be to leverage the EACMS function descriptors noted in FERC Order 848 Paragraph 54 as criteria. This could serve as an approach to assess operational impact and/or functionality of cybersecurity controls that cause a Cyber Security Incident to rise to either level of reportability:

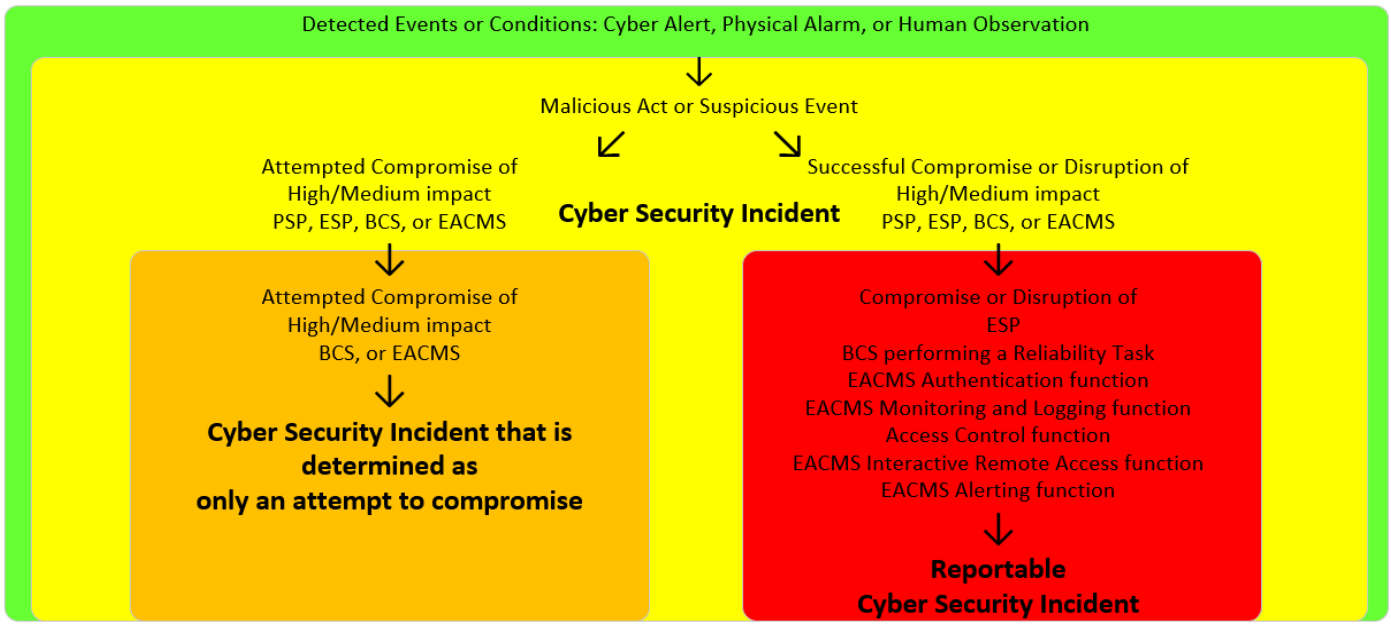


Figure 1 Relationship of Cyber Security Incidents

As shown in the above diagram, there is a progression from identification through assessment and response before a detected event or condition elevates to a reportable level.

First, the Registered Entity must determine the condition meets the criteria for a Cyber Security Incident.

Once the response and assessment has led to a Registered Entity's determination that events or conditions meet the definition of Cyber Security Incident, additional evaluation occurs to establish if established criteria or thresholds have been met for the Registered Entity to determine the Cyber Security Incident qualifies for one of the two reportable conditions:

1. Reportable Cyber Security Incident.
2. Only an attempt to compromise one or more systems identified in the "Applicable Systems" column for Requirement R4 Part 4.2 (pursuant to Responsible Entity processes and established attempt criteria documented in accordance with Requirement R1 Part 1.2)

Once the response and investigation has led to a Registered Entity's determination that the Cyber Security Incident has targeted or impacted the BCS performing reliability tasks and/or cybersecurity functions of the Applicable Systems, associated Cyber Assets, and/or perimeters, the notification and reporting timeframes and obligations begin. Note: Initial (or preliminary) notification is needed within the specified timeframe after this determination, even if required attributes (functional impact, level or intrusion,

attack vector) are not yet known.

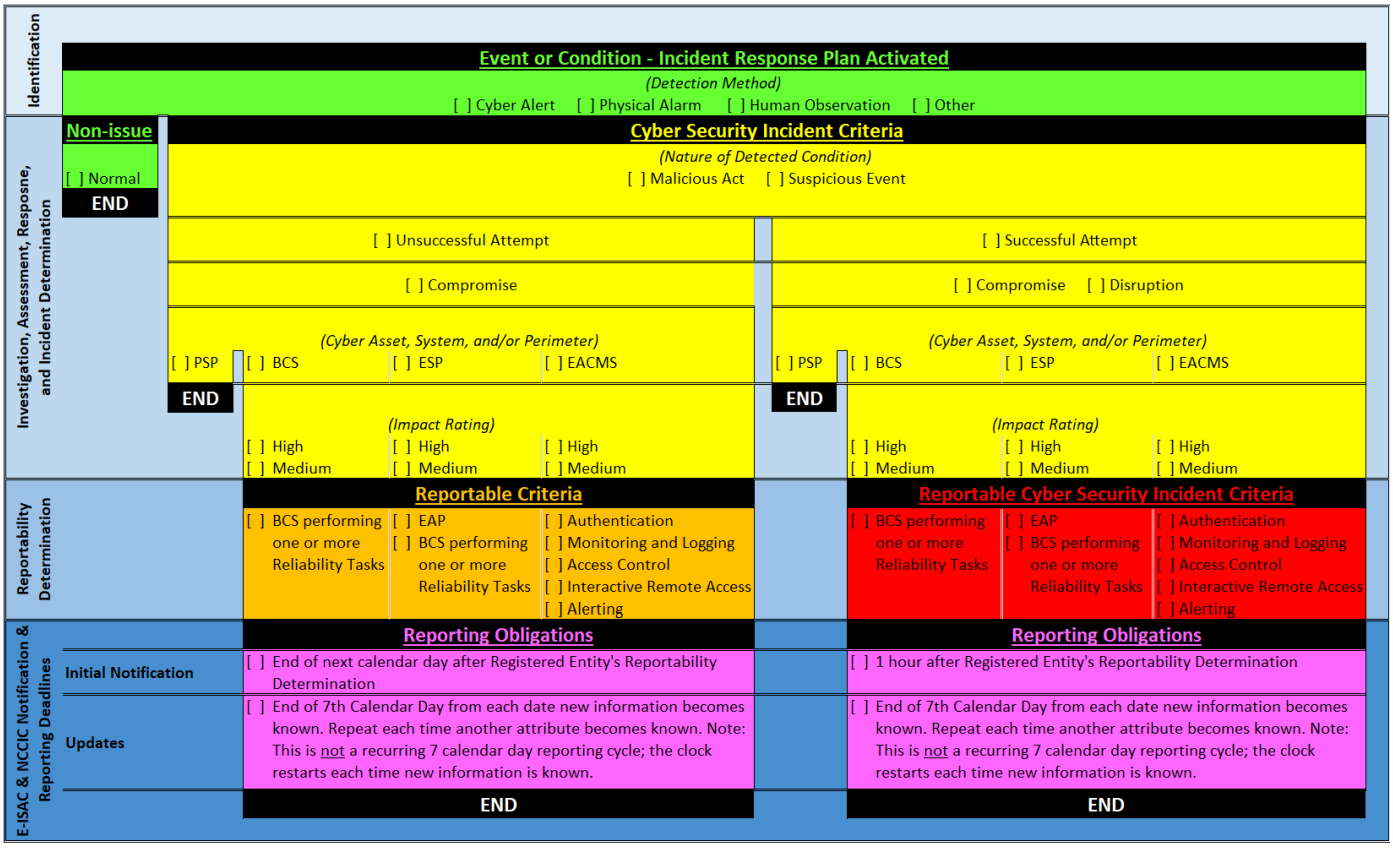
Once this initial notification is made, if all attribute were known, they should have been included in the initial notification and the reporting obligation ends.

If all attributes were not known by the time the initial notification had to be made, the update timeframes trigger from the time the next attribute(s) is learned/known.

A Registered Entity's reporting obligations are met once known information for the three required attributes is reported to E-ISAC and NCCIC, either during the initial notification or subsequently through one or more updates made commensurate with the reporting timeframes.

Determination and Classification of Cyber Security Incidents

Registered Entities may want to consider developing tools illustrating established process criteria that must be met, by definition, as well as the impacted/targeted operational task/cybersecurity functions considered to reach each incident classification and reporting threshold. The below decision tree is one potential approach Registered Entities could employ as a tool to assess events and make the Registered Entity determinations according to process(es) and established criteria documented pursuant to Requirement R1 Parts 1.1 and 1.2.



*Where 'Calendar Day' is used, the 'end' of the day = 11:59 PM local time of that day.
** Where 'Determination' is used, this refers to the Registered Entity's Determination.

Figure 2 Potential Approach Tool

A second potential approach could be a flow diagram illustrating an entity's criteria and determination process as depicted in the example below:

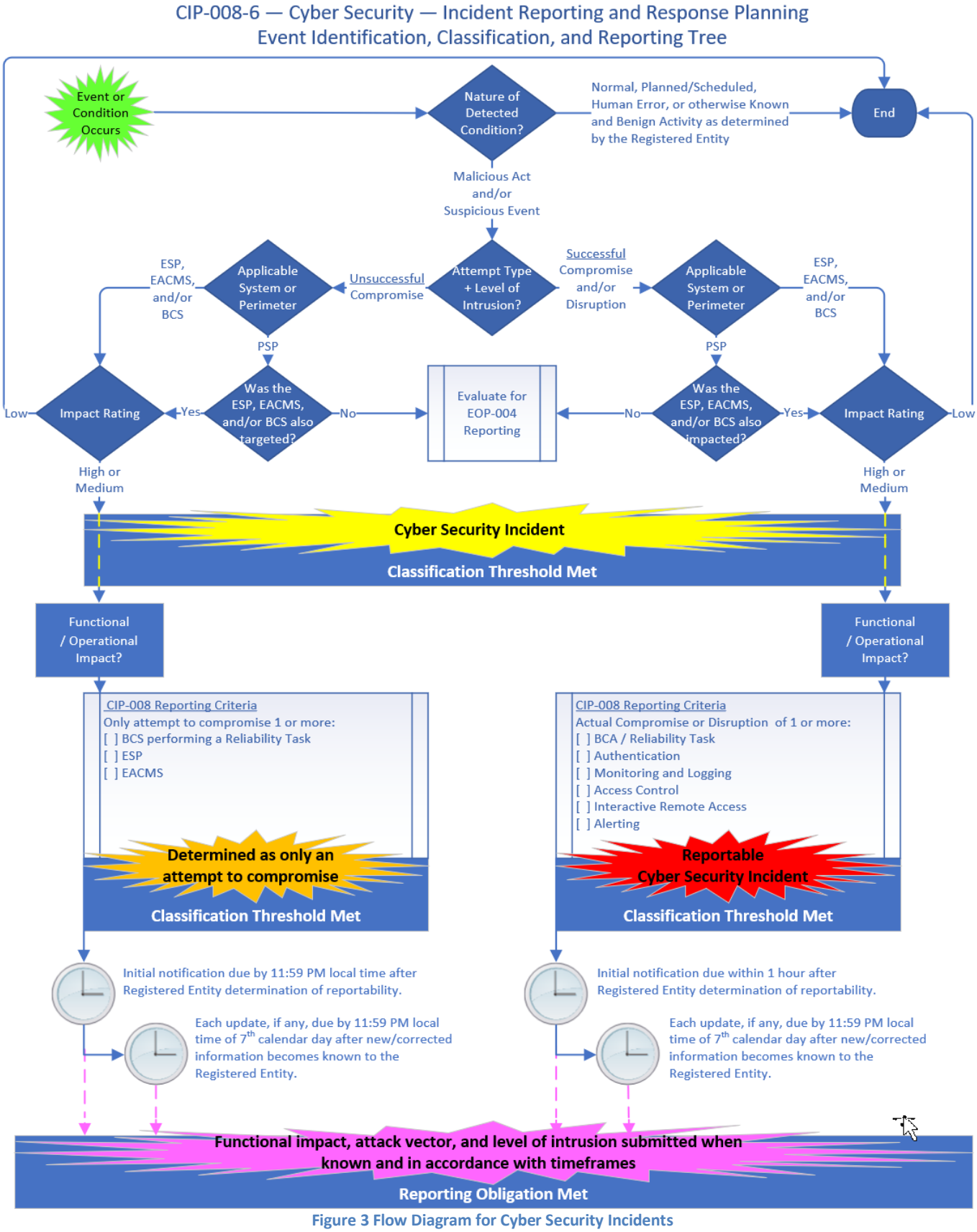


Figure 3 Flow Diagram for Cyber Security Incidents

Example of a Cyber Incident Classification Process

Entities may use a risk analysis-based method for the classification of cyber incidents and determination of Cyber Security Incidents, Reportable Cyber Security Incidents or, Cyber Security Incidents that attempted to compromise a system identified in the "Applicable Systems" column for the Part. The risk analysis-based approach allows entities the flexibility to customize the appropriate response actions for their situation without being administratively burdened by a one size fits all solution. Entities also have the flexibility to incorporate their existing incident management processes which may already define how they classify and determine cyber incidents.

A risk-based approach considers the number of cyber security related event occurrences, the probability that the events will have an impact on their facilities, and severity of the impact of the event. This allows the entity to decide when cyber events should be investigated as cyber incidents, the classification of cyber incidents and the determination of when a cyber incident should be reported; either as part of a voluntary action, as part of a Reportable Cyber Security Incident or a Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for the Part.

Entities should also consider that appropriate reporting of cyber incidents helps other entities in similar situations. The reporting of the details of an incident serves to alert other entities so they may increase their vigilance and take timely preventive or mitigating actions. All entities stand to benefit from such shared information in the long run.

As an example, a typical infrastructure installation is depicted in Figure below.

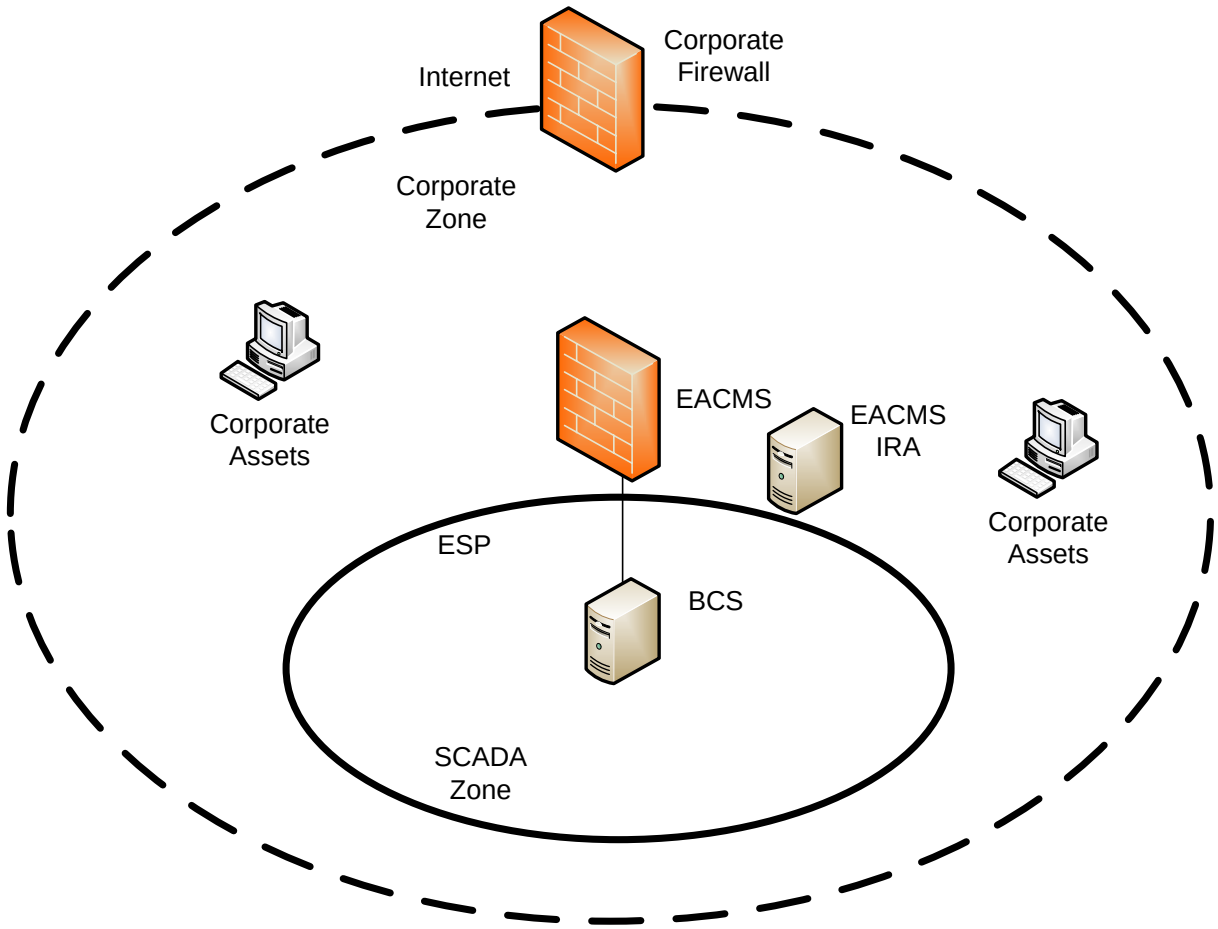


Figure 4 Typical Infrastructure

- A SCADA security zone consists of BES Cyber System (BCS), behind an Electronic Security Perimeter (ESP). The Electronic Access Point (EAP) is an interface of the SCADA firewall which is an Electronic Access Control or Monitoring System (EACMS).

- A Corporate security zone consists of regular corporate assets and other EACMS such as Intermediate Remote Access (IRA) systems. A corporate firewall protects the corporate assets against intrusions from the Internet. The SCADA security zone is nested inside the Corporate security zone.

Sample Classification Schema

A risk analysis could produce the incident categories below:

- Regular cyber events that represent a normal level of events where no further investigation is required such as random port-scans.
- Low risk incidents may be cyber events that become cyber incidents because they are beyond the normal level of events and require some type of investigation. Cyber incidents that are blocked at a firewall and found not to be malicious or suspicious could fall into this category.
- Medium risk incidents may be those cyber incidents that the entity has determined were malicious or suspicious and required mitigation activities.

  Note that while these cyber incidents were malicious or suspicious, they might not meet the definition of a Cyber Security Incident because the entity investigated and determined that the target was not a BCS, ESP, PSP or EACMS.

  For example, a corporate asset infected with well-known corporate malware and, as a result, is scanning the network to find other corporate assets. Although this activity is also being seen at the SCADA firewall (EACMS), the entity investigated and determined that this activity was not a Cyber Security Incident.
- High risk incidents may be those cyber incidents that the entity has determined were malicious or suspicious and did meet the definition of Cyber Security Incidents. For example, malicious malware on a corporate asset that repeatedly attempts to log into a SCADA IRA Intermediate System but is unsuccessful. This would be a Cyber Security Incident and should also fall into the entity's definition of a Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for the Part with the target being an EACMS (SCADA IRA Intermediate System).
- Severe risk incidents may be those Cyber Security Incidents that involves successful compromise of an ESP or EACMS and hence meet the criteria for Reportable Cyber Security Incident. These may also escalate into Cyber Security Incidents that attempted to compromise a system identified in the "Applicable Systems" column for the Part such as the BCS.
- Emergency risk incidents may be those Cyber Security Incidents that compromised or disrupted a BCS that performs one or more reliability tasks of a functional entity. These incidents may represent an immediate threat to BES reliability and may require emergency actions such as external assistance.

These incident categories can be mapped into a standard incident classification and reporting schema like the NCCIC Cyber Incident Scoring System[5]. This is a common schema used by the United States Federal Cybersecurity Centers for describing the severity of cyber incidents and is available to industry to leverage.

Utilizing the NCCIC schema as a basis for identification and classification of Cyber Security Incidents could produce the schema below for application to CIP-008-6:

	General Definition	Observed Actions	Consequences
Level 5 Emergency Black	A Cyber Security Incident that has compromised or disrupted a BCS that performs one or more reliability tasks of a functional entity.	Effect	Incidents that result in imminent threat to public safety and BES reliability. REPORTABLE
Level 4 Severe	A Cyber Security Incident involving a compromise or disruption of an ESP or EACMS; OR Cyber Security Incidents that attempted to compromise a system identified in the "Applicable Systems" column for the Part such as a BCS.	Presence or Possible Effect	Cyber Security Incidents that have the potential to result in a threat to public safety and BES reliability if malicious or suspicious activity continues or escalates. Immediate mitigation is required. REPORTABLE
Level 3 High Orange	Cyber Security Incident that attempted to compromise an EACMS.	Presence	An attempt to compromise an EACMS does not result in a threat to public safety or BES reliability, but still requires mitigation. REPORTABLE
Level 2 Medium Yellow	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.	Engagement	A cyber incident that does not represent a threat to public safety or BES reliability, even though it is malicious or suspicious and required mitigation.
Level 1 Low Green	A cyber incident that investigation found was not malicious or suspicious.	Engagement	A cyber incident that does not represent a threat to public safety.
Level 0 Baseline	Inconsequential cyber events.	Preparation	Cyber events that require no investigation and are not cyber incidents. These do not represent a threat to public safety.

Figure 5 Example of Classification Schema

Reliability tasks may be those tasks that a Responsible Entity determines are associated with the BES Reliability Operating Services (BROS) listed in the NERC Functional Model within Attachment 1 of CIP-002.

[5] https://www.us-cert.gov/NCCIC-Cyber-Incident-Scoring-System

Examples of the use of the Sample Classification Schema

Some examples of the use of the classification schema are listed below. The event number corresponds to the events depicted in the subsequent figures

Type of Event (Event number)	Detection method	Mitigation	Cyber incident that requires investigation	Meets attributes of Cyber Security Incident	Meets attributes of Reportable Cyber Security Incident OR Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for the Part	Comments
External firewall scan (N1)	External IPS log Review of F/W log	External IPS Corporate F/W rules	No	No	No	Determined by entity as regular background activity
Corporate Zone internal scan by non-malicious source (existing network monitoring Tool) (N2)	Corporate IPS Review of EACMS – IRA host F/W Log (CIP-007 R4)	Corporate IPS EACMS IRA Host F/W	No	No	No	Determined by entity as regular background activity – previously investigated and determined to be known source
Corporate Zone internal scan by unknown source (N3)	Corporate IPS Review of EACMS IRA host F/W Log	Corporate IPS IRA EACMS Host F/W	Yes	No	No	Investigation found new network monitoring tool. Added to regular background activity

Type of Event (Event number)	Detection method	Mitigation	Cyber incident that requires investigation	Meets attributes of Cyber Security Incident	Meets attributes of Reportable Cyber Security Incident OR Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for the Part	Comments
Corporate Zone Internal scan by unknown source (N4)	Corporate IPS Corporate Antivirus Review of EACMS IRA host F/W Log Review of EACMS SCADA F/W Log	Corporate IPS IRA EACMS Host F/W Corporate Anti-virus SCADA F/W EACMS	Yes	No	No	Investigation by entity determined malware in Corporate zone that was targeting other corporate assets and not the applicable systems. (via the entity's criteria to evaluate and define attempts to compromise)
Corporate Zone Internal scan by unknown source followed by EACMS IRA login attempts (N5)	Corporate IPS Review of EACMS IRA host F/W Log Review of EACMS IRA failed Logins (CIP-007 R4)	Corporate IPS EACMS host F/W EACMS login 2 factor	Yes	Yes EACMS – IRA targeted	Yes Cyber Security Incidents that attempted to compromise a system identified in the "Applicable Systems" column for the Part	Investigation found malware in Corporate zone that was an attempt to compromise one or more applicable systems - IRA Intermediate System - EACMS (via the entity's criteria to evaluate and define attempts to compromise) **REPORTABLE**

Type of Event (Event number)	Detection method	Mitigation	Cyber incident that requires investigation	Meets attributes of Cyber Security Incident	Meets attributes of Reportable Cyber Security Incident OR Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for the Part	Comments
Corporate Zone Internal scan by unknown source followed by successful EACMS IRA login and attempted BCS logins (N6)	SCADA IPS log Review of EACMS IRA host Logins (CIP-007 R4) Review of BCS failed Logins (CIP-007 R4)	SCADA IPS (CIP-005 R1.5) BCS user/ password login	Yes	Yes	Yes EACMS – IRA host compromised or disrupted Reportable Cyber Security Incident BCS host failed logins Cyber Security Incidents that attempted to compromise a system identified in the "Applicable Systems" column for the Part such as BCS	Investigation found malware that compromised or disrupted EACMS IRA. **REPORTABLE** Attempt to compromise a BCS (via the entity's criteria to evaluate and define attempts to compromise) **REPORTABLE**

Type of Event (Event number)	Detection method	Mitigation	Cyber incident that requires investigation	Meets attributes of Cyber Security Incident	Meets attributes of Reportable Cyber Security Incident OR Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for the Part	Comments
BCS – SCADA system failure following Corporate Zone Internal scan by unknown source, successful EACMS IRA login and successful BCS login (N7)	SCADA system log Review of EACMS IRA host Logins (CIP-007 R4) Review of BCS Logins (CIP-007 R4)	None	Yes	Yes	Yes Comprise or disruption of a BCS performing one or more reliability tasks of a functional entity Reportable Cyber Security Incident	Investigation found malware that compromised a BCS performing one or reliability tasks of a functional entity **REPORTABLE**

Figure 6 Examples of the Use of the Classification Schema

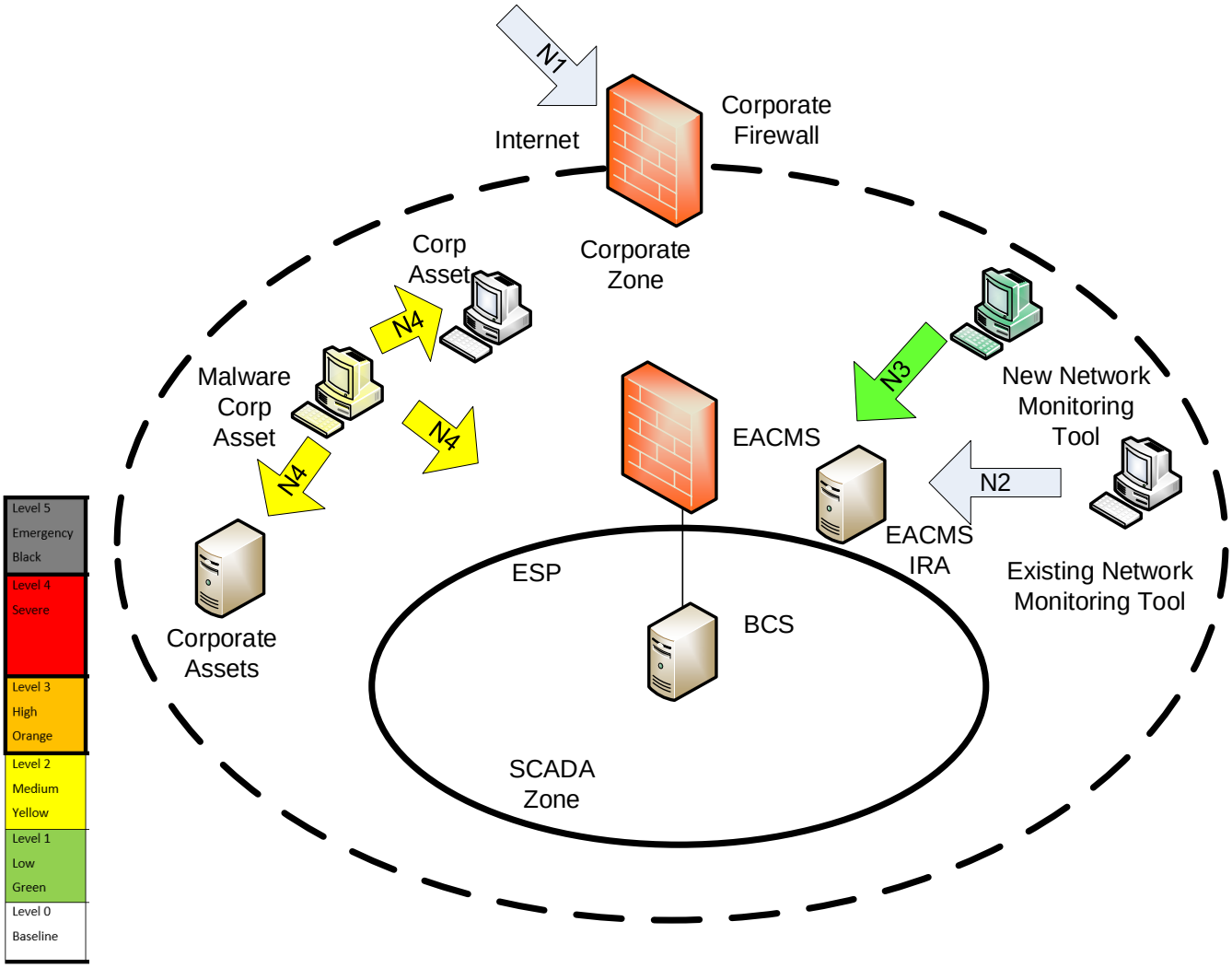


Figure 7 Examples of Non-Reportable Cyber Incidents

The figure above depicts examples of non-reportable cyber incidents using the sample classification schema and examples in Figure 6.

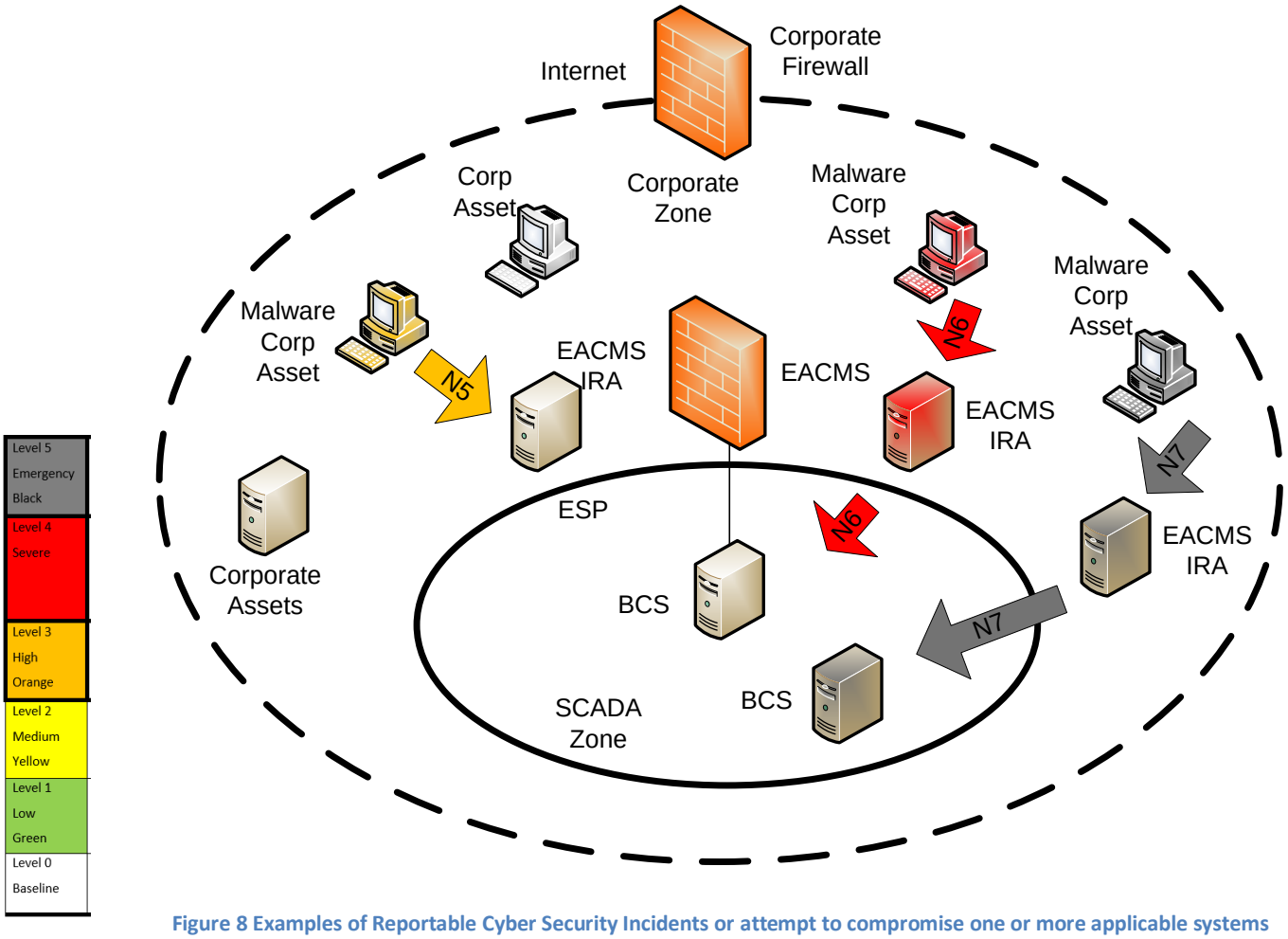


Figure 8 Examples of Reportable Cyber Security Incidents or attempt to compromise one or more applicable systems

The figure above depicts examples of Reportable Cyber Security Incidents or attempts to compromise one or more systems identified in the "Applicable Systems" column for the Part using the sample classification schema and examples in Figure 6.

Attempts to Compromise and Cyber Security Incidents

Registered Entities may want to evaluate and document what is normal within their environment to help scope and define network communications and activity that may constitute 'an attempt to compromise' in the context of CIP-008. This can help aid Subject Matter Experts (SMEs) in identifying deviations from normal, and could significantly assist a Registered Entity in timely and effective Incident determination, response, and vital information sharing. Since no two Registered Entities are alike, it stands to reason that interpretations and perspectives may vary.

Registered Entities are encouraged to explore options and tools designed to that take the guess work out of the process without being so overly prescriptive as to create undue administrative burden or remove needed discretion and professional judgment from the SMEs.

It is up to the Registered Entity to determine what constitutes and 'attempt to compromise', and this should be documented through the establishment of criteria that is incorporated into the Registered Entity's process. Once established, Registered Entities may want to consider incorporating a checklist to apply the defined set of criteria for SMEs to leverage as a part of the process to determine reportability.

As an example, a Registered Entity could define an "attempt to compromise" as an act with malicious intent to gain access or to cause harm to the normal operation of a Cyber Asset in the "Applicable Systems" column. Using this sample definition:

a. Actions that are **not** an attempt to compromise an applicable Cyber Asset/System electronically are:
   i. A Registered Entity's own equipment scanning a Cyber Asset for vulnerabilities or to verify its existence that is performed expected on demand or on an approved periodic schedule.
   ii. Broadcast traffic as part of normal network traffic. A firewall may block and log this traffic, but it does not have malicious intent.
   iii. Attempts to access a Cyber Asset by an authorized user that have been determined to fail due to human error.

b. Actions that **are** an attempt to compromise an applicable Cyber Asset/System electronically are:
   i. Scanning a Cyber Asset for vulnerabilities or to verify its existence that is not approved by the Registered Entity's management nor process(es). This could be from an entity's own equipment due to an upstream compromise or malware.
   ii. 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.
   iii. Attempts to escalate privileges on a Cyber Asset by an authorized user that has been determined to fail due to not being authorize for that privilege level.

Registered Entities may also want to evaluate system architecture for ways to limit exposure for 'attempts to compromise'. Techniques like the implementation of security zones and/or network segmentation can minimize the level of traffic that can get to applicable Cyber Assets and help minimize the attack surface.

Registered Entities with implementations that involve an Electronic Access Control or Monitoring System (EACMS) containing both an Electronic Access Point (EAP) and a public internet facing interface are strongly encouraged to change this configuration in favor of architectures that offer layers of safeguards and a defense in depth approach.

Similarly, Registered Entities with implementations that involve an EACMS containing both an EAP and a corporate facing interface to their business networks may also want to consider options to re-architect to reduce cyber events from the corporate environment such as broadcast storms from causing extra administrative workload.

Examples of Cyber Security Incidents, attempts to compromise "Applicable Systems", and Reportable Cyber Security Incidents

The table below contains examples of various degrees of events or conditions at varied levels of determination:

Event	Normal or Benign	Malicious / Confirmed Suspicious
PSP breach	• Unauthorized user compromises the PSP to steal copper and the Registered Entity determines cybersecurity controls were not targeted and remain in place.	• Unauthorized user breaks into a Substation control house (**CIP-006-6 R1.5 activates BES Cyber Security Incident response plan within 15 minutes of detection.**)
		• Unauthorized user breaks into a Substation control house and inserts unauthorized Removable Media into an EACMS or BCS and the Registered Entity determines no interaction between the USB and the EACMS or BCS occurred. (**Cyber Security Incident pursuant to CIP-008-6 R1.1 determination**)
	• An equipment operator loses control of a backhoe and crashes into a control house, breaching the PSP and the Registered Entity determines it was accidental, cybersecurity controls were not targeted and remain in place.	• Registered Entity determines the unauthorized Removable Media contains malware (**determination of only an attempt to compromise one or more systems identified in the "Applicable Systems" column for CIP-008-6 R1.2**)
		• Registered Entity determines the malware has harvested the credentials of a BCS, gained unauthorized access and disrupted a reliability task. (**Reportable Cyber Security Incident pursuant to CIP-008-6 R1.2 determination**)
Port Scanning	• Registered Entity owned monitoring tool that runs scheduled periodic scans to detect deviations from baseline is scanning an EACMS or BCS at the expected time.	• Registered Entity owned monitoring tool that normally runs scheduled periodic scans to detect deviations from baseline is scanning an EACMS or BCS at an unexpected time and the Registered Entity has determined this as suspicious. (**Cyber Security Incident pursuant to CIP-008-6 R1.1 determination**)
	• A Registered Entity performs a port scan of an EACMS or BCS during a scheduled Cyber Vulnerability Assessment activity.	• Registered Entity owned monitoring tool that normally runs scheduled periodic scans to detect deviations from baseline is repeatedly scanning an EACMS or BCS and the Registered Entity determines it is targeting specific ports relevant to the BCS. (**determination of only an attempt to compromise one or more systems identified in the "Applicable Systems" column for CIP-008-6 R1.2**)
		• Registered Entity owned monitoring tool that normally runs scheduled periodic scans to detect deviations from baseline is repeatedly scanning an EACMS or BCS and the Registered Entity determines it gained unauthorized access to the EACMS or BCS. (**Reportable Cyber Security Incident pursuant to CIP-008-6 R1.2 determination**)

Event	Normal or Benign	Malicious / Confirmed Suspicious
Detected malware	• A corporate machine infected by a known Enterprise Windows-specific vulnerability is scanning all local hosts including a non-Windows-based EACMS or BCS and is determined by the Registered Entity to be an SMB exploit applicable to only Windows-based machines.	• An infected corporate machine is scanning all local hosts including an EACMS or BCS for well-known ports and determined to be a suspicious event by the Registered Entity. (**Cyber Security Incident pursuant to CIP-008-6 R1.1 determination**)
		• An infected corporate machine is scanning all local hosts including an EACMS or BCS for specific known ICS ports. (**determination of only an attempt to compromise one or more systems identified in the "Applicable Systems" column for CIP-008-6 R1.2**)
		• An infected corporate machine is scanning all local hosts including an EACMS or BCS for specific known ICS ports and has attempted to gain unauthorized access to the EACMS or BCS. (**determination of only an attempt to compromise one or more systems identified in the "Applicable Systems" column for CIP-008-6 R1.2**)
		• An infected corporate machine is scanning all local hosts including an EACMS or BCS for specific known ICS ports and exploited/compromised specified ICS ports that perform command and control functions of a BCS. (**Reportable Cyber Security Incident pursuant to CIP-008-6 R1.2 determination**)
Login activity	• Authorized user exceeded the Registered Entity defined threshold (CIP-007-6 R5.7) for unsuccessful login attempts against an EACMS or BCS and the Registered Entity confirmed the user incorrectly entered his/her password after performing annual password changes.	• Unknown individual attempts to login to a known default account on an EACMS or BCS with a publicly known default password, and the Registered Entity investigates that activity as a Cyber Security Incident deems suspicious. (**Cyber Security Incident pursuant to CIP-008-6 R1.1 determination**).
	• A system exceeds the Registered Entity defined threshold (CIP-007-6 R5.7) for unsuccessful login against an EACMS or BCS and locks out a system account and the Registered Entity confirmed the system account's password had changed but the accessing application/service had not yet been updated to use the new password.	• Unknown individual attempts to login to a known default account on an EACMS or BCS with a publicly known default password, and the Registered Entity's investigation determines that activity is being initiated from an external IP address and it continues aggressively with additional passwords and failed login attempts. (**determination of only an attempt to compromise one or more systems identified in the "Applicable Systems" column for CIP-008-6 R1.2**).
		• Unknown individual attempts to login to a known default account on an EACMS or BCS with a publicly known default password, and the Registered Entity's investigation determines that activity is being initiated from an external IP address and it continues aggressively with additional passwords and successfully gains unauthorized access to an EACMS or BCS. (**Reportable Cyber Security Incident pursuant to CIP-008-6 R1.2 determination**).

Figure 9 Examples of Cyber Security Incidents, attempts to compromise "Applicable Systems", and Reportable Cyber Security Incidents

Example of Sample Criteria to Evaluate and Define Attempts to Compromise

An entity may establish criteria to evaluate and define attempts to compromise based on their existing capabilities and facilities associated with the other CIP Standards.

The sample criteria listed below are examples and are not intended to be exhaustive.

CIP-005 R1.5:

Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.

Sample criteria:
Where investigation by entity was not able to determine that the source of the following was not suspicious and/or malicious:

- Detected known malicious or suspected malicious communications for both inbound and outbound communications.

CIP-005 R2.1:

Require multi-factor authentication for all Interactive Remote Access sessions.

Sample criteria:
Where investigation by entity was not able to determine that the source of the following was not suspicious and/or malicious:

- Repeated attempts to authenticate using multi-factor authentication

CIP-007 R4.1:

Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events:

4.1.1. Detected successful login attempts;
4.1.2. Detected failed access attempts and failed login attempts;
4.1.3. Detected malicious code.

Sample criteria:
Where investigation by entity was not able to determine that the source of the following was not suspicious and/or malicious:

- Successful login attempts outside of normal business hours
- Successful login attempts from unexpected personnel such as those who are on vacation or medical leave
- Detected failed access attempts from unexpected network sources
- Detected failed login attempts to default accounts
- Detected failed login attempts from authorized personnel accounts exceeding X per day

- Detected failed login attempts from authorized personnel accounts where the account owner was not the source
- Detected malicious code on applicable systems

CIP-007 R5.7:

Where technically feasible, either:

- *Limit the number of unsuccessful authentication attempts; or*
- *Generate alerts after a threshold of unsuccessful authentication attempts.*

Sample criteria:
Where investigation by entity was not able to determine that the source of the following was not suspicious and/ or malicious:

- Account locked due to limit of unsuccessful authentication attempts exceeded more than X times per day
- Threshold of unsuccessful authentication attempts exceeds more than X every Y minutes

CIP-010 R2.1:

Monitor at least once every 35 calendar days for changes to the baseline configuration (as described in Requirement R1, Part 1.1). Document and investigate detected unauthorized changes.

Sample criteria:
Where investigation by entity was not able to determine that the source of the following was not suspicious and/ or malicious:

- Detected unauthorized changes to the baseline configuration

An entity may establish additional criteria to evaluate and define attempts to compromise based on their infrastructure configuration:

Sample criteria:
Where investigation by entity determines that the specific activity, while malicious or/and suspicious:

- Attempt to compromise was not intended to target the “Applicable Systems”

Requirement R1

R1. *Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include each of the applicable requirement parts in CIP-008-6 Table R1 – Cyber Security Incident Response Plan Specifications. [Violation Risk Factor: Lower] [Time Horizon: Long Term Planning].*

1.1. One or more processes to identify, classify, and respond to Cyber Security Incidents.

1.2. One or more processes:

1.2.1. Establish criteria to evaluate and define attempts to compromise;

- Determine if an identified Cyber Security Incident is A Reportable Cyber Security Incident or
- Only an attempt to compromise one or more systems identified in the "Applicable Systems" column for this Part; and

1.2.2. Provide notification per Requirement R4.

1.3. The roles and responsibilities of Cyber Security Incident response groups or individuals.

1.4. Incident handling procedures for Cyber Security Incidents.

General Considerations for R1

Preserved CIP-008-5 Version History from Guidelines and Technical Basis

An enterprise or single incident response plan for all BES Cyber Systems may be used to meet the Requirement.

The following guidelines are available to assist in addressing the required components of a Cyber Security Incident response plan:

- *Department of Homeland Security, Control Systems Security Program, Developing an Industrial Control Systems Cyber Security Incident Response Capability, 2009, online at* ***http://www.us-cert.gov/control_systems/practices/documents/final-RP_ics_cybersecurity_incident_response_100609.pdf***
- *National Institute of Standards and Technology, Computer Security Incident Handling Guide, Special Publication 800-61 revision 1, March 2008, online at* ***http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf***

For Part 1.2, a Reportable Cyber Security Incident is a Cyber Security Incident that has compromised or disrupted one or more reliability tasks of a functional entity. It is helpful to distinguish Reportable Cyber Security Incidents as one resulting in a necessary response action.

A response action can fall into one of two categories: Necessary or elective. The distinguishing characteristic is whether or not action was taken in response to an event. Precautionary measures that are not in response to any persistent damage or effects may be designated as elective. All other response actions to avoid any persistent damage or adverse effects, which include the activation of redundant systems, should be designated as necessary.

Implementation Guidance for R1

Process to Identify, Classify, and Respond to Cyber Security Incidents (R1.1, R1.2)

The figure below is an example of a process that is used to identify, classify and respond to Cyber Security Incidents. This process uses the sample classification schema shown earlier that the entity uses to identify and classify Cyber Security Incidents as well as the sample criteria to evaluate and define attempts to compromise, if they are Reportable Cyber Security Incidents or Cyber Security Incidents that attempted to compromise a system identified in the "Applicable Systems" column for the Part.

This process is adapted from those related to the Information Technology Infrastructure Library (ITIL). ITIL is a set of detailed practices for IT service management (ITSM) that focuses on aligning IT services with the needs of business.

Note: There is recognition that the organizational structure and resource composition is unique to each entity and that roles and responsibilities may vary. The process diagram to follow is no intended to be prescriptive, and instead constitutes merely one potential approach where the assignments/functions in the cross functional swim lanes could be tailored to meet the unique needs of any entity.

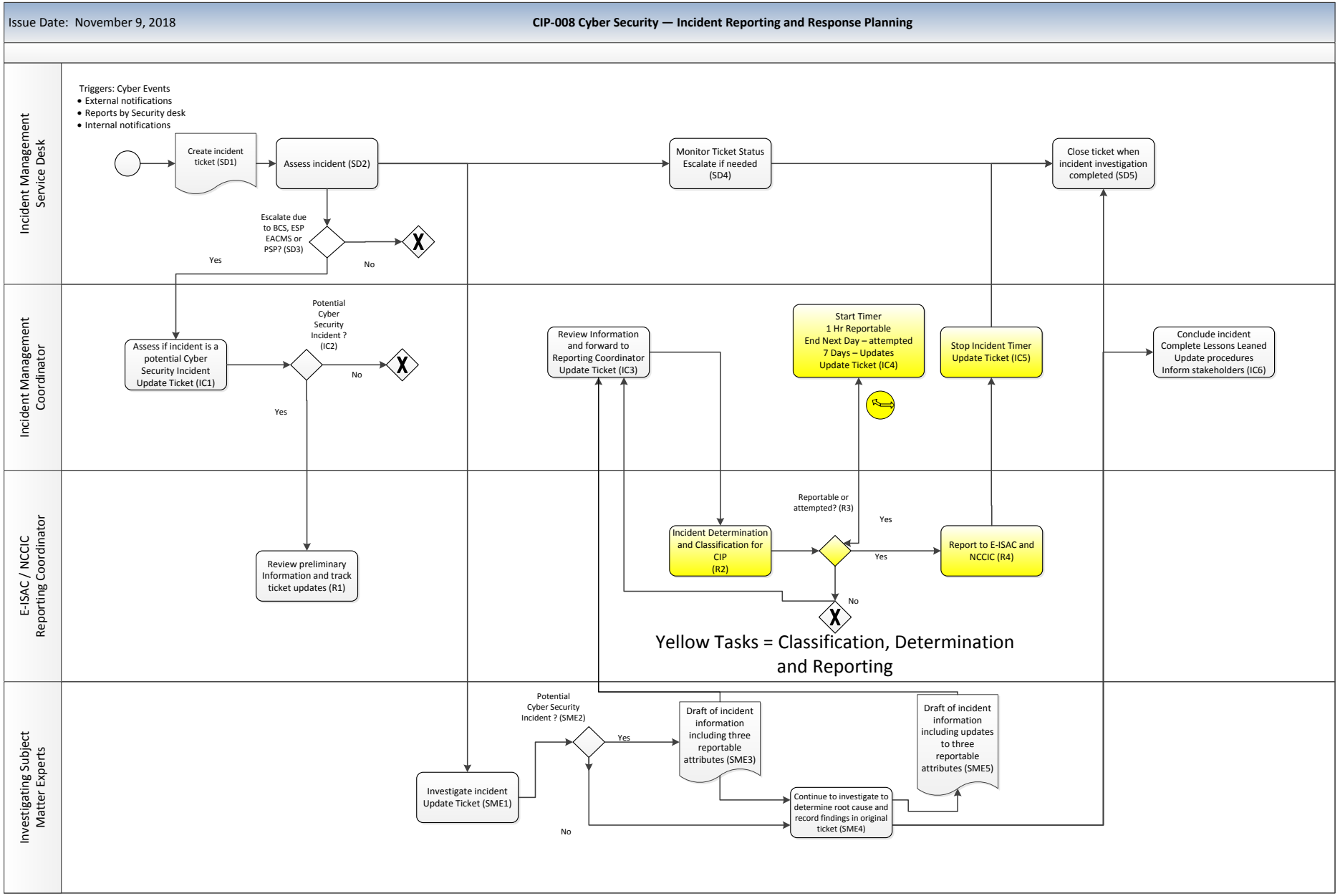


Figure 10 Sample Process to Identify, Classify and Respond to Cyber Security Incidents

Supporting Narrative Description of Sample Process to Identify, Classify, and Respond to Cyber Security Incidents (R1.1, R1.2)

1. The Incident Management Service Desk identifies that a cyber event that requires investigation has occurred.
2. Incident Management Service Desk creates an incident ticket to log the suspected cyber incident (SD1).
3. Incident Management Service Desk performs initial assessment of the suspected cyber incident and performs any initial triage or service restoration as needed (SD2).
4. If the suspected cyber incident involves BES Cyber Systems (BCS), Electronic Access Control or Monitoring Systems (EACMS), Electronic Security Perimeter (ESP) or Physical Security Perimeters (PSP), the Incident Management Service Desk will escalate the incident to an Incident Management Coordinator whom will act as the coordinator until the incident is closed (SD3)
5. The Incident Management Coordinator performs a secondary initial assessment to determine if the incident has the potential to be a Cyber Security Incident, a Reportable Cyber Security Incident, or a Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for the Part.

   They update the incident ticket, assigning the appropriate Investigating Subject Matter Experts (IC1).
6. If the Incident Management Coordinator determines that the incident has the potential to be reportable, the E-ISAC/ NCCIC Reporting Coordinator is alerted and copied on the information contained in the incident ticket. The E-ISAC/ NCCIC Reporting Coordinator continues to monitor the updates to the incident ticket (IC2)
7. The Incident Management Service Desk ensures the assigned Investigating SMEs are notified, and the incident ticket information is updated (SD2, SD4)
8. The assigned SMEs investigate the incident ticket updating with the Incident Management Coordinator as appropriate (SME1). The Incident Management Coordinator will monitor the progress of the investigation and assign additional SMEs or escalate as needed.
9. If initial investigation by SMEs finds that the incident may be a Cyber Security Incident and has the potential to be reportable (SME2), the SMEs will inform the Incident Management Coordinator and forward the known information including the required three attributes (SME3). Attributes which are unknown at the current time will be reported as "unknown".
10. The SMEs will continue their investigation to determine the root cause of the incident, performing triage or service restoration as needed, continue to investigate the three required attributes and update incident ticket information (SME4).
11. If the incident is found to be potentially reportable, the Incident Management Coordinator reviews the information, adds any details collected by other investigating SMEs and resolves any missing information as needed. The information is forwarded to the E-ISAC/ NCCIC Reporting Coordinator (IC3)
12. The E-ISAC/ NCCIC Reporting Coordinator reviews the information received, performs classification of the incident (R2). They determine if the incident is a Cyber Security Incident and determine if it is either a Reportable Cyber Security Incident or Cyber Security Incident that attempted to compromise

a system identified in the "Applicable Systems" column for the Part. The information to be reported is finalized (R3).

13. Upon determination that the incident is reportable, E-ISAC/ NCCIC Reporting Coordinator informs the Incident Management Coordinator to begin a clock timer set to the appropriate time frame (IC4) and performs the required notification including the three required attributes. The incident ticket is updated with the incident classification and determination time for compliance evidence purposes:
    - Within 1 hour for initial notification of Reportable Cyber Security Incident,
    - By end of the next day for a Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for the Part,
    - Within 7 calendar days of determination of new or changed attribute information required in Part 4.1

14. The E-ISAC/ NCCIC Reporting Coordinator informs the Incident Management Coordinator when notification is completed and time that the notifications occurred at. The Incident Management Coordinator will stop the appropriate timer and updates the incident ticket with the appropriate information for compliance evidence purposes (IC5)
15. If Incident Management Coordinator that has not received confirmation of notification, they may escalate, as needed, prior to expiry of the applicable timer. Upon expiry of the timer, the Incident Management Coordinator must inform the CIP Senior Manager (IC4)
16. During the continued investigation of the incident (SME4), the SMEs may find that an update of any of the three required attributes is potentially required. The SMEs will inform the Incident Management Coordinator and forward a draft of the updated information (SME5)
17. The Incident Management Coordinator reviews the draft update information including adding other details, and then informs E-ISAC/ NCCIC Reporting Coordinator, forwarding the potential update information (IC3)
18. The E-ISAC/ NCCIC Reporting Coordinator reviews the potential updated information and determines if the update to any of the three required attributes is reportable (R3).
19. Upon determination that the update is reportable, E-ISAC/ NCCIC Reporting Coordinator informs the Incident Management Coordinator to begin a timer set to the appropriate time frame (i.e. 7 calendar days). The incident ticket is updated with the determination time for compliance evidence purposes (IC4)
20. The E-ISAC/ NCCIC Reporting Coordinator updates both E-ISAC and NCCIC with the information associated with any of the three required attributes (R4)
21. The E-ISAC/ NCCIC Reporting Coordinator informs the Incident Management Coordinator that the update to E-ISAC and NCCIC is completed and times that the updates occurred at. The Incident Management Coordinator will stop the appropriate timer and update the incident ticket with the appropriate information for compliance purposes (IC5)

22. If the Incident Management Coordinator that has not received confirmation of the update being completed, prior to the expiration of the timer, they may escalate as needed. Upon expiry of the timer, the Incident Management Coordinator must inform the CIP Senior Manager (IC4)
23. Upon closure of the incident, the Incident Management Coordinator will ensure that the last reportable update to the three required attributes accurately reflects the closure information. If a further update of the three required attributes is required, the Incident Management Coordinator will inform the appropriate Subject Matter Expert to initiate an update (SME5).
24. The Incident Management Coordinator informs the Incident Management Service Desk that the incident ticket may be closed (SD5).
25. The Incident Management Coordinator will initiate a "Lessons Leaned" session and update to the Cyber Incident Reporting and Response Plan and any other documentation, procedures, etc. within 90 days (IC6). They will inform all stakeholders of any updates to the Cyber Incident Reporting and Response Plan and any other applicable documentation

Roles and Responsibilities (R1.3)

In the example process, the defined Roles and Responsibilities are as follows, but can be tailored by any entity to align with their unique organization:

- Incident Management Service Desk is responsible for initial activities, incident ticketing and incident logging:
    - Initial identification, categorization and prioritization,
    - Initial diagnosis and triage/service restoration,
    - Initial assignment of incident tickets to Investigating Subject Matter Experts (SMEs)
    - Initial escalation to an Incident Management Coordinator upon assessment (if needed)
    - Monitoring incident ticket status and initiating further escalation (if needed)
    - Incident ticket resolution and closure
    - General incident status communication with the user community

- Incident Management Coordinator is responsible for the over-all coordination of activities related to an assigned incident:
    - Detailed assignment of tasks to Investigating SMEs
    - Ensure that all assigned activities are being performed in a timely manner
    - Ensuring regulatory reporting time limits are met and initiating escalation if needed
    - Communicating incident status with major affected stakeholders
    - Coordinating with the Incident Management Service Desk to update incident tickets with status and the logging of required details and assisting them to perform general incident status communications with the user community

- Coordinating with the E-ISAC/NCCIC Reporting Coordinator for cyber incidents with the potential of being Cyber Security Incidents, Reportable Cyber Security Incidents or Cyber Security Incidents that attempted to compromise a system identified in the "Applicable Systems" column for the Part. Assisting the E-ISAC/NCCIC Reporting Coordinator with information to aid in the classification of the cyber incident.
- Escalation as needed according to the priority and severity of the issue
- Coordination of service restoration and incident closure
- Coordination of incident review following closure of incidents, identification of potential problems and documenting the "Lessons Learned"
- Initiating update of processes or procedures as needed and communicating the updates to stakeholders

- E-ISAC/ NCCIC Reporting Coordinator is responsible for the coordination of regulatory reporting activities such as those related to E-ISAC and NCCIC:
  - Review of completeness incident information for classification and reporting purposes
  - Incident classification for reporting purposes
  - Determination if this incident is a Cyber Security Incident, Reportable Cyber Security Incident or a Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for the Part
  - Completeness of the required three attributes to be reported
  - Notification to E-ISAC and NCCIC and submission of the three required attributes
  - Coordinating with Incident Management Coordinator to ensure timing is in accordance with regulatory requirements and that incident logging is complete for compliance evidence purposes

- Investigating Subject Matter Experts are responsible for detailed technical tasks related to the investigation of the incident and performing the needed recovery actions:
  - Perform investigation tasks related to the incident as assigned by the Incident Management Coordinator to determine the root cause of the incident
  - Perform service restoration tasks related to the incident as assigned
  - Update incident ticket and ensure all required details are logged
  - Obtaining information on the three required attributes for both initial notification and updates
  - After incident closure, participate in "Lessons Learned" sessions and update procedures as needed

Incident handling procedures for Cyber Security Incidents (R1.4)

Each of the defined roles in the example process may have specific procedures covering various aspects of their tasks being accomplished within the process. The sample process documents "what" the overall required steps are whereas the procedures document "how" each step is carried out:

- Incident Management Service Desk Procedures:
    - Procedures of when to classify cyber events as possible cyber incidents
    - Procedures to determine if BCS, PSP, ESP or EACMS are involved and decision criteria of when to escalate to an Incident Management Coordinator.
    - Procedures for initial diagnosis, triage and service restoration
    - Procedures for incident ticketing, assignment, escalation and closure

- Incident Management Coordinator Procedures:
    - Procedures for finding if cyber events or incidents could be possible Cyber Security Incidents, Reportable Cyber Security Incidents or Cyber Security Incidents that attempted to compromise a system identified in the "Applicable Systems" column for the Part. These potential incidents require notification to the E-ISAC/ NCCIC Coordinator
    - Procedures for the assignment and tracking of tasks to Investigating SMEs
    - Procedures associated with regulatory reporting time limits
    - Procedures for incident review, documentation of lessons learned, tracking of completion of documentation update status
- E-ISAC/ NCCIC Reporting Coordinator Procedures:
    - Procedures on how to use the Entity's own classification and reporting schema to classify cyber incidents and determine Cyber Security Incidents, Reportable Cyber Security Incidents or Cyber Security Incidents that attempted to compromise a system identified in the "Applicable Systems" column for the Part
    - Procedures on the review of information to be used for reporting the three required attributes to be included for E-ISAC or NCCIC notification including the handling of any BES Cyber System Information
    - Procedures for the notification of updates to E-ISAC and NCCIC including the submission of the three required attributes
- Investigating Subject Matter Experts Procedures:
    - Procedures for the classification of cyber incidents to possible Cyber Security Incidents, possible Reportable Cyber Security Incidents or possible Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for the Part and the required information needed to be obtained.
    - Procedures for troubleshooting tasks to determine root cause of an incident

- Procedures for service restoration tasks after an incident
- Procedures for triggering the forensic preservation of the incident
- Procedures on when updates are necessary to information on the required attributes associated with a Reportable Cyber Security Incident or a Cyber Security Incident that attempted to compromise a system identified in the “Applicable Systems” column for the Part

Requirement R2

R2. *Each Responsible Entity shall implement each of its documented Cyber Security Incident response plans to collectively include each of the applicable requirement parts in CIP-008-6 Table R2 – Cyber Security Incident Response Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-Time Operations]*

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.

2.2. Use the Cyber Security Incident response plan(s) under Requirement R1 when responding to a Reportable Cyber Security Incident, Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for the 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.

2.3. 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.

General Considerations for R2

Preserved CIP-008-5 Version History from Guidelines and Technical Basis

If a plan is written at a high enough level, then every action during the response should not be subject to scrutiny. The plan will likely allow for the appropriate variance in tactical decisions made by incident responders. Deviations from the plan can be documented during the incident response or afterward as part of the review.

For more specific types of exercises, refer to the FEMA Homeland Security Exercise and Evaluation Program (HSEEP). It lists the following four types of discussion-based exercises: seminar, workshop, tabletop, and games. In particular, it defines that, "A tabletop exercise involves key personnel discussing simulated scenarios in an informal setting. Table top exercises (TTX) can be used to assess plans, policies, and procedures."

The HSEEP lists the following three types of operations-based exercises: Drill, functional exercise, and full-scale exercise. It defines that, "[A] full-scale exercise is a multi-agency, multi-jurisdictional, multi-discipline exercise involving functional (e.g., joint field office, Emergency operation centers, etc.) and 'boots on the ground' response (e.g., firefighters decontaminating mock victims)."

In addition to the requirements to implement the response plan, Part 2.3 specifies entities must retain relevant records for Reportable Cyber Security Incidents. There are several examples of specific types of

evidence listed in the measure. Entities should refer to their handling procedures to determine the types of evidence to retain and how to transport and store the evidence. For further information in retaining incident records, refer to the NIST Guide to Integrating Forensic Techniques into Incident Response (SP800-86). The NIST guideline includes a section (Section 3.1.2) on acquiring data when performing forensics.

Implementation Guidance for R2

Acceptable Testing Methods

The SDT made no changes to the testing requirements located in Requirement Parts 2 and 3. The applicable system expansion to include EACMS was the only change. The SDT purposefully did not expand the acceptable testing methods to include an actual response to a Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for the Part. This was based on incident risk level and benefits of exercising the full response plan(s).

Annual testing of the incident response plan(s) are important because they may reveal weaknesses, vulnerabilities, and opportunity for improvement. The current test options include: a paper drill (coordinated tabletop exercise), an operational exercise (a full-scale, multiple entity exercise), and actual response to a Reportable Cyber Security Incident.

All of these options, especially the latter, involve a complete, step-by-step run-through of the plan components. Many problems that would occur in a real incident also will be present in the test exercise or drill[6]. In fact, it is recommended that drills and exercises go to the extreme and simulate worst-case scenarios.

Conversely, a Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for the Part, may only exercise several components and would likely not result in the same level of response action. Cyber Security Incidents that attempted to compromise an applicable system, by their very nature, have less risk than an actual compromise. A Responsible Entity's actual response to unauthorized access attempts and suspicious activities does not rise to the same level of required response that actual disruption of a BCS performing one or more reliability tasks would. For these reasons, the SDT did not change the acceptable testing methods of a response plan(s), and using records associated to attempts to compromise are not sufficient evidence to demonstrate compliance with the 15-month testing requirements.

The sample process in Requirement R1.1 shows how an actual Reportable Cyber Security Incident is documented using the entity's incident management system including how each role defined in Requirement R1.3 updates the incident ticket. The incident ticket is a permanent record of the incident including any actions undertaken. The Incident Management Coordinator is responsible for documenting deviations from the Cyber Incident response plan and initiating any corrections required in the process or documentation for meeting the Requirement. In addition, to assure sufficient evidence, records should be dated and should include documentation that sufficiently describes the actual or simulated scenario(s), response actions, event identifications and classifications, the application of Cyber Security Incident and reportability criteria, reportability determinations, and reporting submissions and timeframes.

[6] 2009, Department of Homeland Security, Developing an Industrial Control Systems Cybersecurity Incident Response Capability, page 13.

Requirement R3

R3. *Each Responsible Entity shall maintain each of its Cyber Security Incident response plans according to each of the applicable requirement parts in CIP-008-6 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication. [Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

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.

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.

General Considerations for R3

Preserved CIP-008-5 Version History from Guidelines and Technical Basis

The process of conducting lessons learned can involve the response team discussing the incident to determine gaps or areas of improvement within the plan. Any documented deviations from the plan from Part 2.2 can serve as input to the lessons learned. It is possible to have a Reportable Cyber Security Incident without any documented lessons learned. In such cases, the entity must retain documentation of the absence of any lessons learned associated with the Reportable Cyber Security Incident.

Entities should consider meeting with all of the individuals involved in the incident and documenting the lessons learned as soon after the incident as possible. This allows more time for making effective updates to the plan, obtaining any necessary approvals, and distributing those updates to the incident response team.

This may include changes to the names or contact information listed in the plan. Technology changes affecting the plan may include referenced information sources, communication systems or ticketing systems.

Implementation Guidance for R3

The sample process in Requirement R1.1 shows how an actual Reportable Cyber Security Incident results in an update to Cyber Security Incident response plan, incorporating the "lessons learned". The role of Incident Management Coordinator includes the responsibility for meeting Requirement R3. Registered Entities should assure updated plans are dated in demonstration of the timelines mandated by Requirement R3. It may help to append these records to the dated Lessons Learned from an actual response or an exercise to test the plan to further demonstrate plan update timelines were met and relevant areas of the plan were updated to align with the outcomes and conclusions in the Lessons Learned.

Requirement R4

R4. Each Responsible Entity shall notify the Electricity Information Sharing and Analysis Center (E-ISAC) and, if subject to the jurisdiction of the United States, the United States National Cybersecurity and Communications Integration Center (NCCIC), or their successors, of a Reportable Cyber Security Incident and a Cyber Security Incident that was an attempt to compromise a system identified in the "Applicable Systems" column, unless prohibited by law, in accordance with each of the applicable requirement parts in *CIP-008-6 Table R4 – Notifications and Reporting for Cyber Security Incidents*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

4.1. 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. 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. Provide updates within 7 calendar days of determination of new or changed attribute information required in Part 4.1

General Considerations for R4

Registered Entities may want to consider designing tools or mechanisms to assure incident responders have the information needed to efficiently and timely report events or conditions that rise to the level of reportability. A potential approach is to include the E-ISAC/NCCIC phone numbers in response plans, calling trees, or even within corporate directories for ease of retrieval. Another potential approach is to develop a distribution list that includes both entities so one notification can easily be sent at the same time. Certainly, Registered Entities should consider implementing secure methods for transit if using email. Another approach could be to incorporate website URLs into processes to have them at hand. Finally, for Registered Entities that prefer to leverage secure portals for E-ISAC or NCCIC, advance planning by having individual user portal accounts requested, authorized, configured, and tested is encouraged ad can be a time saver in emergency situations.

Implementation Guidance for R4

The sample process in Requirement R1.1 shows how initial notification and updates of the required attributes is performed within the specified time lines (yellow colored tasks).

For attributes that are not known, these should be reported as "unknown"

NCCIC Reporting

NCCIC reporting guidelines for reporting events related to Industrial Control Systems can be found here:

https://ics-cert.us-cert.gov/Report-Incident

https://www.us-cert.gov/incident-notification-guidelines

NCCIC prefers the reporting of 10 attributes, although they will accept any information that is shared. A potential mapping between the NCCIC preferred attributes and the attributes required to comply with CIP-008-6 standard could be represented are as follows:

CIP-008-6 Reporting	NCCIC Reporting	Comment
Functional Impact	Identify the current level of impact on agency functions or services (Functional Impact).	
Functional Impact	Identify the type of information lost, compromised, or corrupted (Information Impact).	
Functional Impact	Identify when the activity was first detected.	
Level of Intrusion	Estimate the scope of time and resources needed to recover from the incident (Recoverability).	
Level of Intrusion	Provide any indicators of compromise, including signatures or detection measures developed in relationship to the incident	
Level of Intrusion	Identify the number of systems, records, and users impacted.	
Level of Intrusion	Identify the network location of the observed activity.	
Level of Intrusion	Provide any mitigation activities undertaken in response to the incident.	
Attack Vector	Identify the attack vector(s) that led to the incident.	
Name and Phone	Identify point of contact information for additional follow-up.	

Figure 11 NCCIC Reporting Attributes

Example of a Reporting Form

Entities may wish to create an internal standard form to be used to report Reportable Cyber Security Incidents and Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for the Part. The advantages of using a standard internal form are:

- A standard internal format for the communications of cyber incident information between the various internal roles with respect to obligations of CIP-008-6, Requirement R4
- A standard written record of the notification of the minimum 3 attributes having been reported to E-ISAC and NCCIC in accordance with CIP-008-6, Requirement R4 which can be easily stored, sorted and retrieved for compliance purposes

An example of an internal standard form is shown. The instructions on how to complete this form are included after it.

CIP-008-6 Requirement R4

Cyber Security Incident Reporting Form

This form may be used to report Reportable Cyber Security Incidents and Cyber Security Incidents that were an attempt to compromise a system listed in the "Applicable Systems" column for the Part.

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

☐ Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for the Part

Reporting Category

☐ Initial Notification

☐ Update

Required Attribute Information

1. Attack Vector ☐ Initial ☐ Update

Click or tap here to enter text.

2. Functional Impact ☐ Initial ☐ Update

Click or tap here to enter text.

3. Level of Intrusion ☐ Initial ☐ Update

Click or tap here to enter text.

Instructions for Example of a Reporting Form

These are instructions on how to complete the optional form

CIP-008-6
Cyber Security Incident Reporting Form Instructions

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 report includes information for a Reportable Cyber Security Incident.
	Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for the Part	Check this box if report includes information for a Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for the Part Note: Do not check this box for incidents related solely to a PSP(s).
Reporting Category	**Initial Notification**	Check this box if report is being submitted to satisfy initial notification obligations of Requirement R4 Part 4.2.
	Update	Check this box if report is being submitted to satisfy subsequent follow-up or update obligations of Requirement R4 Part 4.3.
Required Attribute Information (Attack Vector fields)	**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. • If not known, specify 'unknown' in the field. *Examples include, but are not limited to, malware, use of stolen credentials, etc.*

CIP-008-6– Reportable Cyber Security Incident Reporting Form Instructions		
Form Section	**Field Name**	**Instructions**
	Attack Vector Initial Checkbox	If report is being used to provide the preliminary report, select the 'Initial' checkbox.
	Attack Vector Update Checkbox	If report is being used to provide an update report, select the 'Update' checkbox.
Required Attribute Information (Functional Impact fields)	**Functional Impact**	• If known, enter a narrative description of the functional impact for the compromise or attempt to compromise to satisfy the required attribute specified in Requirement R4 Part 4.1. • If not known, specify 'unknown' in the field. *Examples include, but are not limited to, situational awareness, dynamic response, ability to perform Real-time Assessments, or Real-time monitoring etc.*
	Functional Impact Initial Checkbox	If report is being used to provide the preliminary report, select the 'Initial' checkbox.
	Functional Impact Update Checkbox	If report is being used to provide an update report, select the 'Update' checkbox.
Required Attribute Information (Level of Intrusion fields)	**Level of Intrusion**	• If known, enter a narrative description of the level of intrusion for the compromise or attempt to compromise to satisfy the required attribute specified in Requirement R4 Part 4.1. • If not known, specify 'unknown' in the field. *Examples include, but are not limited to, whether the compromise or attempt to compromise occurred on Applicable Systems outside the Electronic Security Perimeter (ESP), at the ESP, or inside the ESP. Additionally, level of intrusion may include the Applicable System impact level and Cyber System classification level.*
	Level of Intrusion Initial Checkbox	If report is being used to provide the preliminary report, select the 'Initial' checkbox.
	Level of Intrusion Update Checkbox	If report is being used to provide an update, select the 'Update' checkbox.