CIP Compliance Monitoring Updates

Emily Stuetzle, CISA
Manager, CIP Compliance

Patrick Palompo, PE
Manager, O&P Compliance

March 26, 2024

• REC

NPCC, Inc.

Agenda

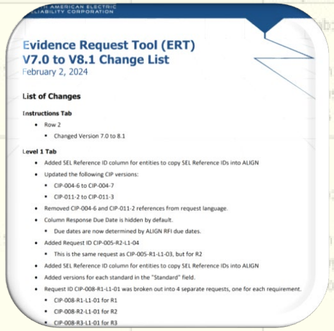
NERC ERT v8.1 Updates

Overview of FERC Staff Report:

“2023 Lessons Learned from Commission-Led CIP Reliability Audits”

Designed by Harryarts / Freepik

NERC ERT v8.1



ORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Evidence Request Tool (ERT)
V7.0 to V8.1 Change List
February 2, 2024

List of Changes

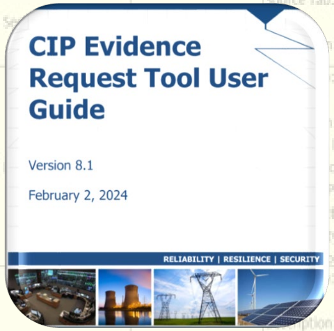
Instructions Tab

- Row 2
  - Changed Version 7.0 to 8.1

Level 1 Tab

- Added SEL Reference ID column for entities to copy SEL Reference IDs into ALIGN
- Updated the following CIP versions:
  - CIP-004-6 to CIP-004-7
  - CIP-011-2 to CIP-011-3
- Removed CIP-004-6 and CIP-011-2 references from request language.
- Column Response Due Date is hidden by default.
  - Due dates are now determined by ALIGN RFI due dates.
- Added Request ID CIP-005-R2-L1-04
  - This is the same request as CIP-005-R1-L1-03, but for R2
- Added SEL Reference ID column for entities to copy SEL Reference IDs into ALIGN
- Added versions for each standard in the "Standard" field.
- Request ID CIP-008-R1-L1-01 was broken out into 4 separate requests, one for each requirement.
  - CIP-008-R1-L1-01 for R1
  - CIP-008-R2-L1-01 for R2
  - CIP-008-R3-L1-01 for R3

V7.0 to v8.1 Change List



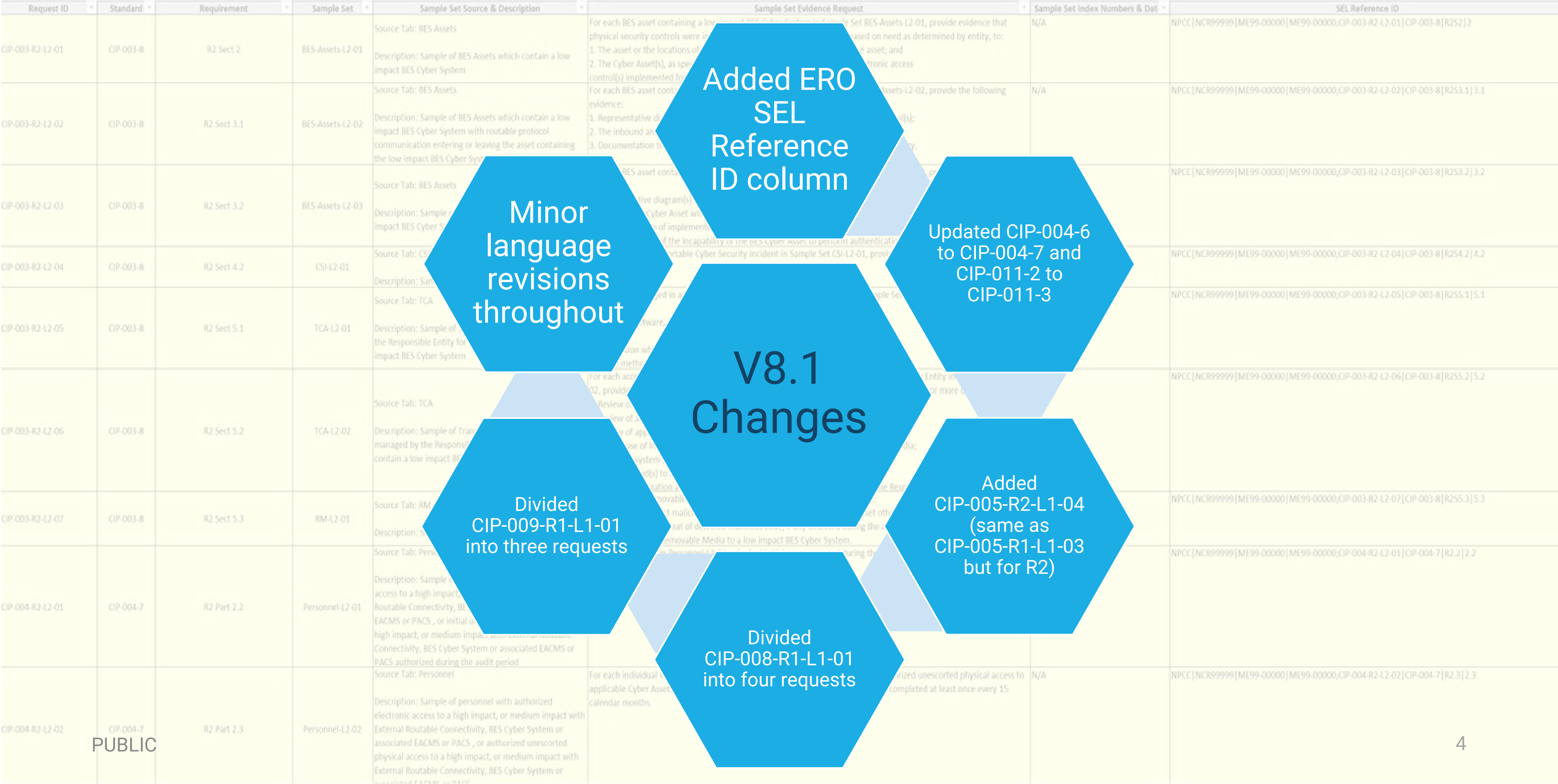
CIP Evidence Request Tool User Guide

Version 8.1

February 2, 2024

RELIABILITY | RESILIENCE | SECURITY

CIP ERT v8.1 User Guide

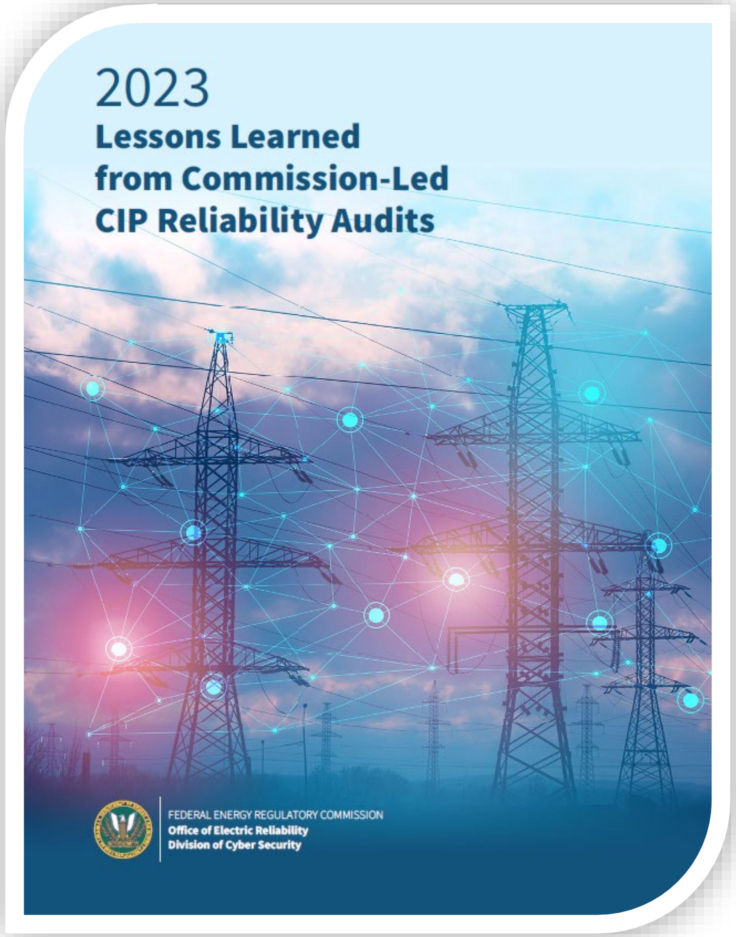


V8.1 Changes

- Added ERO SEL Reference ID column
- Updated CIP-004-6 to CIP-004-7 and CIP-011-2 to CIP-011-3
- Added CIP-005-R2-L1-04 (same as CIP-005-R1-L1-03 but for R2)
- Divided CIP-008-R1-L1-01 into four requests
- Divided CIP-009-R1-L1-01 into three requests
- Minor language revisions throughout

Request ID	Standard	Requirement	Sample Set	Sample Set Index Numbers & Dat	SEL Reference ID
CIP-003-R2-L2-01	CIP-003-8	R2 Sect 2	BES-Assets-L2-01	N/A	NPCC|NCR99999|ME99-00000|ME99-00000,CIP-003-R2-L2-01|CIP-003-8|R2S2|2
CIP-003-R2-L2-02	CIP-003-8	R2 Sect 3.1	BES-Assets-L2-02	N/A	NPCC|NCR99999|ME99-00000|ME99-00000,CIP-003-R2-L2-02|CIP-003-8|R2S3.1|3.1
CIP-003-R2-L2-03	CIP-003-8	R2 Sect 3.2	BES-Assets-L2-03		NPCC|NCR99999|ME99-00000|ME99-00000,CIP-003-R2-L2-03|CIP-003-8|R2S3.2|3.2
CIP-003-R2-L2-04	CIP-003-8	R2 Sect 4.2	CSI-L2-01		NPCC|NCR99999|ME99-00000|ME99-00000,CIP-003-R2-L2-04|CIP-003-8|R2S4.2|4.2
CIP-003-R2-L2-05	CIP-003-8	R2 Sect 5.1	TCA-L2-01		NPCC|NCR99999|ME99-00000|ME99-00000,CIP-003-R2-L2-05|CIP-003-8|R2S5.1|5.1
CIP-003-R2-L2-06	CIP-003-8	R2 Sect 5.2	TCA-L2-02		NPCC|NCR99999|ME99-00000|ME99-00000,CIP-003-R2-L2-06|CIP-003-8|R2S5.2|5.2
CIP-003-R2-L2-07	CIP-003-8	R2 Sect 5.3	RM-L2-01		NPCC|NCR99999|ME99-00000|ME99-00000,CIP-003-R2-L2-07|CIP-003-8|R2S5.3|5.3
CIP-004-R2-L2-01	CIP-004-7	R2 Part 2.2	Personnel-L2-01		NPCC|NCR99999|ME99-00000|ME99-00000,CIP-004-R2-L2-01|CIP-004-7|R2.2|2.2
CIP-004-R2-L2-02	CIP-004-7	R2 Part 2.3	Personnel-L2-02	N/A	NPCC|NCR99999|ME99-00000|ME99-00000,CIP-004-R2-L2-02|CIP-004-7|R2.3|2.3

FERC Staff Report



2023

Lessons Learned from Commission-Led CIP Reliability Audits

FEDERAL ENERGY REGULATORY COMMISSION
Office of Electric Reliability
Division of Cyber Security

- The Federal Energy Regulatory Commission completed CIP Audits of several U.S.-based NERC registered entities
- Staff from NERC and the Regional Entities participated in the CIP Audits, including the virtual and on-site portions
- This report provides information and recommendations to NERC, Regional Entities, and registered entities

Four Lessons Learned

1 - Identify and categorize all BES Cyber Systems and their associated BES Cyber Assets

2 - Ensure reportable Cyber Security Incidents and attempts to compromise that were identified as Cyber Security Incidents are reported to the Electricity Information Sharing and Analysis Center (E-ISAC) and to the Cybersecurity and Infrastructure Security Agency (CISA)

3 - Restrict all inbound and outbound access permissions, including the reason for granting access and denying all other access by default

4 - Enhance supply chain risk management programs to include evaluating the supply chain risks of existing vendors and develop a plan to respond to the risks that are identified

Lessons Learned 1 - CIP-002-5.1a
Identify and categorize all BES Cyber Systems and their associated BES Cyber Assets

Identified Failure

- Some entities did not identify each medium impact BES Cyber System at a single plant location identified by a Reliability Coordinator as critical to the derivation of IROLs and their associated contingencies, as required by Attachment 1, Section 2.6.

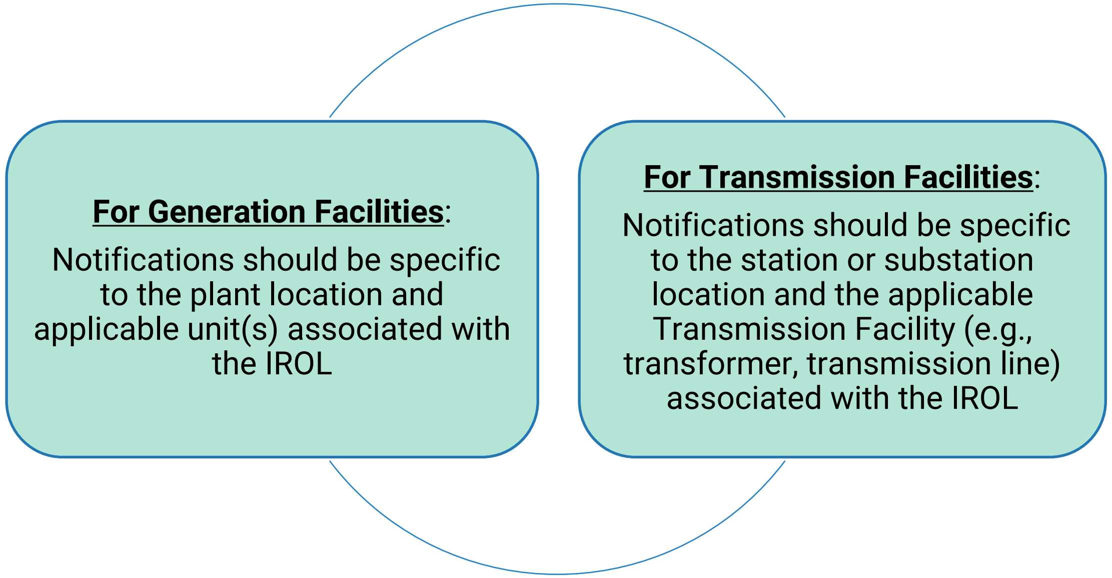
Requirement Language R1.1.2 – Attachment 1 Section 2.6

- Identify each of the medium impact BES Cyber Systems, not included in Section 1, associated with “Generation at a single plant location or Transmission Facilities at a single station or substation location that are identified by its Reliability Coordinator, Planning Coordinator, or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.”

Lessons Learned 1 - CIP-002-5.1a
Identify and categorize all BES Cyber Systems and their associated BES Cyber Assets

Reliability Coordinators (RC), Planning Coordinators (PC), or Transmission Planners (TP)

- **<u>Notify</u>** Generator Owners (GO) and/or Transmission Owners (TO) that their “Generation or Transmission Facility” is critical to the derivation of any Interconnection Reliability Operating Limits (IROLs) and their associated contingencies



<u>For Generation Facilities</u>:

Notifications should be specific to the plant location and applicable unit(s) associated with the IROL

<u>For Transmission Facilities</u>:

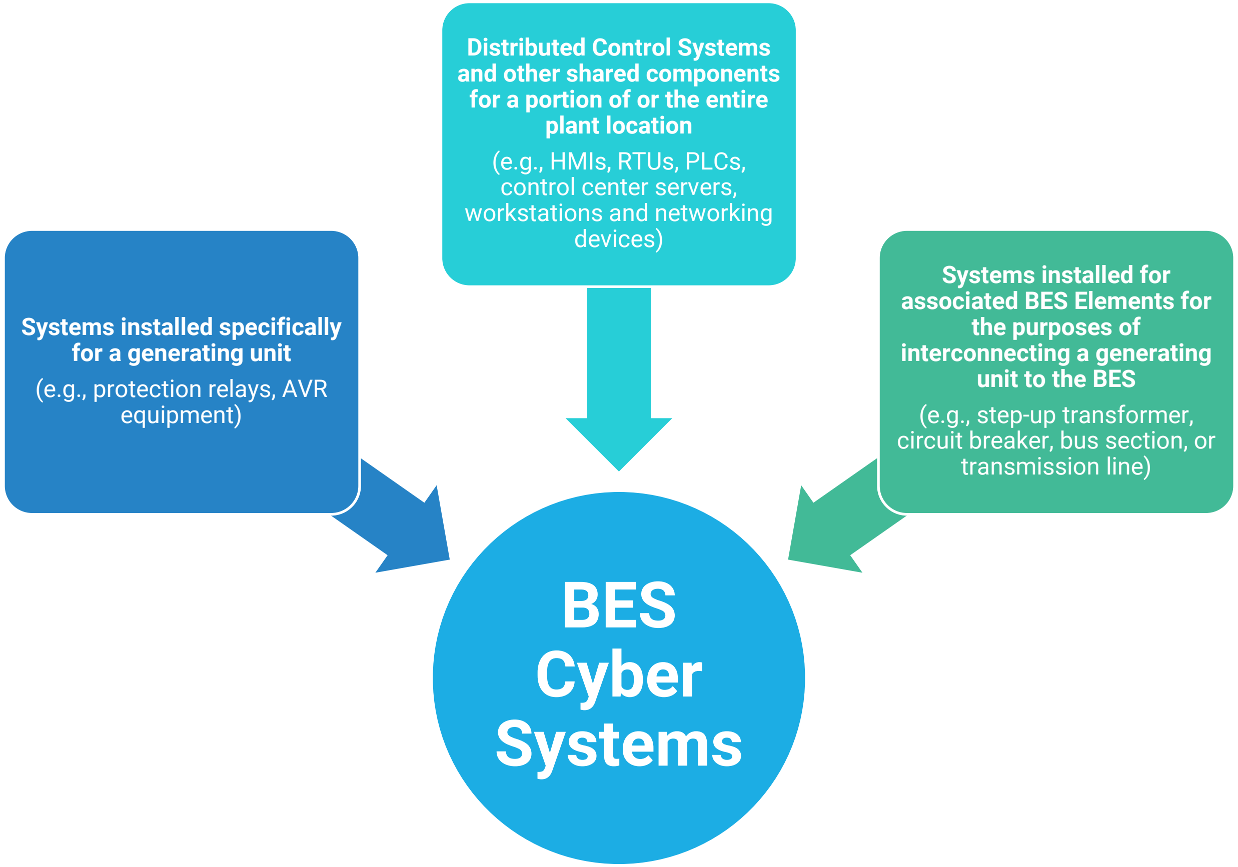
Notifications should be specific to the station or substation location and the applicable Transmission Facility (e.g., transformer, transmission line) associated with the IROL

Specific BES Cyber Systems pertaining to the specific Generation or Transmission Facility are left to the GO or TO for identification and categorization

Lessons Learned 1 - CIP-002-5.1a
Identify and categorize all BES Cyber Systems and their associated BES Cyber Assets

Generator Owners

- **<u>Upon notification</u>** that you have specific Generation Facilities applicable to the derivation of an IROL:
  - Identify and categorize all BES Cyber Systems and associated BES Cyber Assets that are associated with the specific Generation Facility



Distributed Control Systems and other shared components for a portion of or the entire plant location

(e.g., HMIs, RTUs, PLCs, control center servers, workstations and networking devices)

Systems installed specifically for a generating unit

(e.g., protection relays, AVR equipment)

Systems installed for associated BES Elements for the purposes of interconnecting a generating unit to the BES

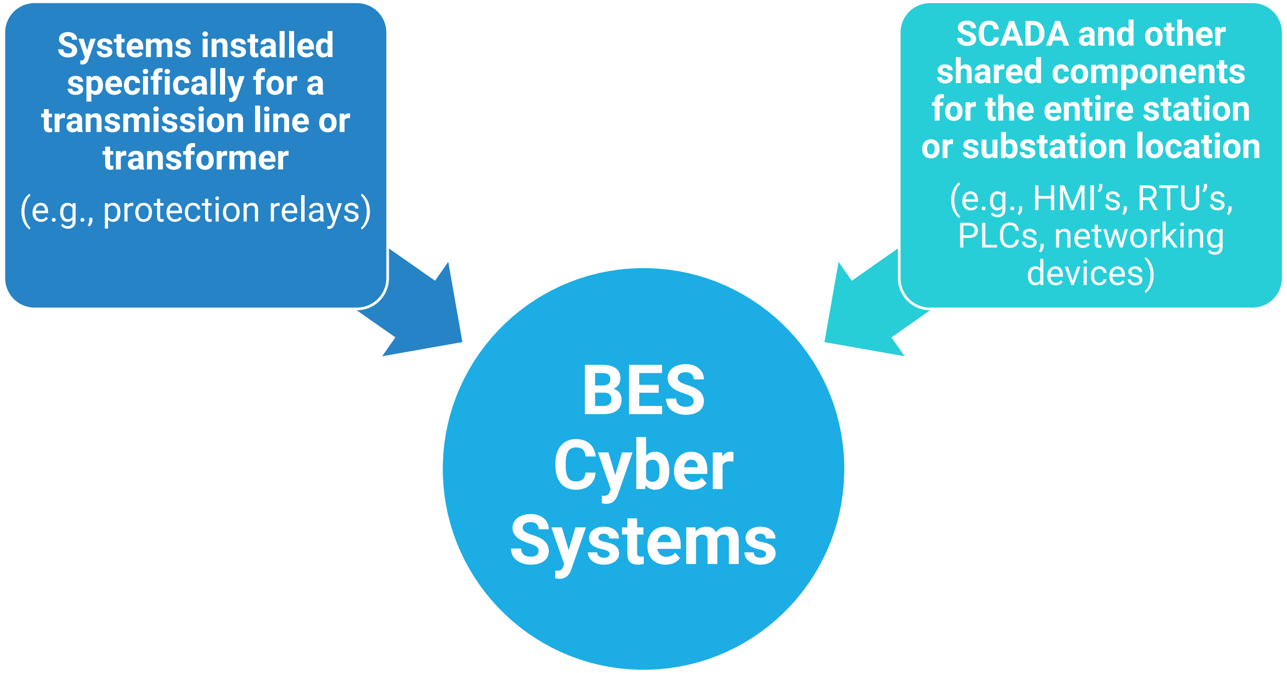
(e.g., step-up transformer, circuit breaker, bus section, or transmission line)

BES Cyber Systems

Lessons Learned 1 - CIP-002-5.1a
Identify and categorize all BES Cyber Systems and their associated BES Cyber Assets

Transmission Owners

- **<u>Upon notification</u>** that you have specific Transmission Facilities applicable to the derivation of an IROL:
  - Identify and categorize all BES Cyber Systems and associated BES Cyber Assets that are associated with the specific Transmission Facility



Systems installed specifically for a transmission line or transformer

(e.g., protection relays)

SCADA and other shared components for the entire station or substation location

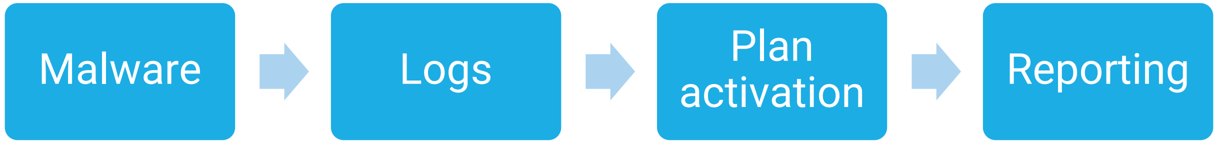
(e.g., HMI's, RTU's, PLCs, networking devices)

BES Cyber Systems

Lessons Learned 2 - CIP-003-8 R2 Section 4, CIP-007-6 R4, CIP-008-6 R4 Ensure reportable Cyber Security Incidents and attempts to compromise that were identified as Cyber Security Incidents are reported to Electricity Information Sharing and Analysis Center (E-ISAC) and Cybersecurity and Infrastructure Security Agency (CISA)

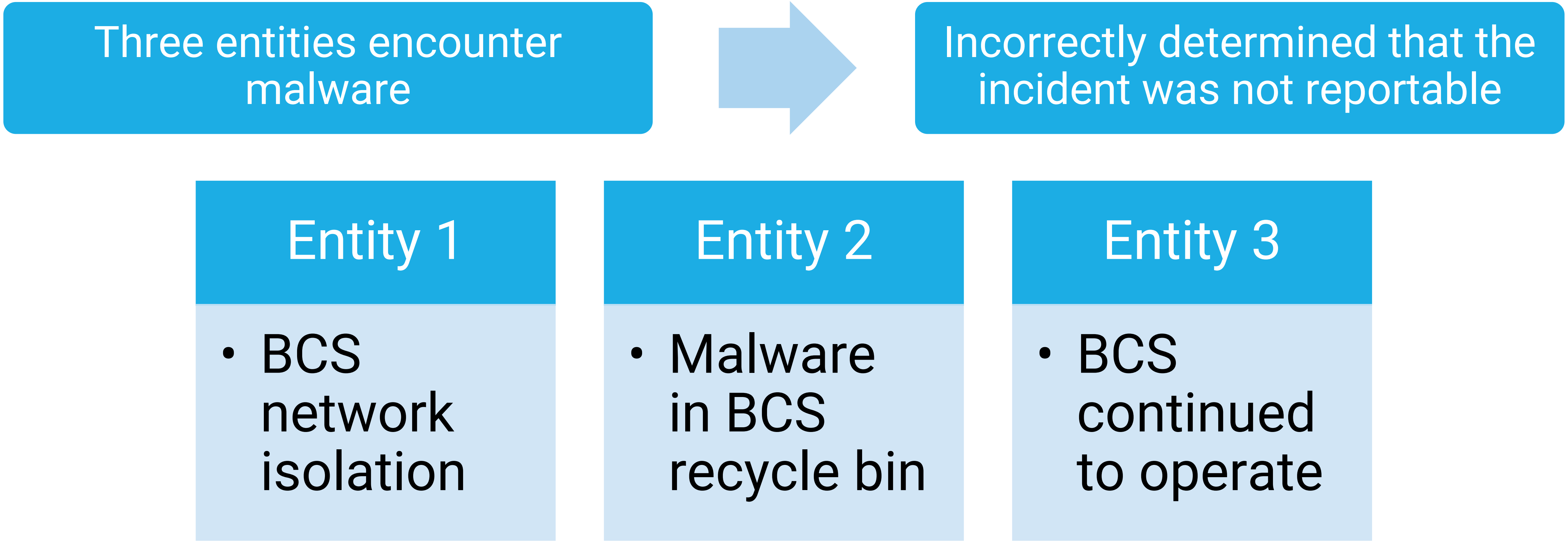
Cyber Security Incident Response Plan

- **<u>Compromise or attempt to compromise</u>**
  - Potential security events required by Reliability Standard CIP-007-6, Requirement R4



Malware → Logs → Plan activation → Reporting

Lessons Learned 2 - CIP-003-8 R2 Section 4, CIP-007-6 R4, CIP-008-6 R4
Ensure reportable Cyber Security Incidents and attempts to compromise that were identified as Cyber Security Incidents are reported to Electricity Information Sharing and Analysis Center (E-ISAC) and Cybersecurity and Infrastructure Security Agency (CISA)



Three entities encounter malware

Incorrectly determined that the incident was not reportable

Entity 1

- BCS network isolation

Entity 2

- Malware in BCS recycle bin

Entity 3

- BCS continued to operate

Lessons Learned 3 - CIP-005-7, R1.3
Restrict all inbound and outbound access permissions, including the reason for granting access and denying all other access by default

Unrestricted Internet Control Message Protocol usage

No documented justifications for communications

Overly permissive access permissions

No ‘deny all’

Lessons Learned 3 - CIP-005-7, R1.3
Restrict all inbound and outbound access permissions, including the reason for granting access and denying all other access by default

FERC recommendations:

- Ensure all access permissions are accounted for
- Review policies quarterly
- Block IPv6 at the network border

Lessons Learned 4 - CIP-013-1, R1
Enhance supply chain risk management programs to include evaluating the supply chain risks of existing vendors and develop a plan to respond to the risks that are identified

Multiple entities did not properly implement their supply chain risk management plans

Plans did not include processes to respond to identified risks, specifically for “grandfathered’ contracts

Recommend entities voluntarily apply CIP-013 to agreements that pre-date the standard.

Lessons Learned 4 - CIP-013-1, R1
Enhance supply chain risk management programs to include evaluating the supply chain risks of existing vendors and develop a plan to respond to the risks that are identified

FERC identified best practices

- Prioritize vendors based on risk
- Identify the vendor’s country
- Ensure all purchases go through reviews that include a cybersecurity review
- Implement controls for purchasing IT equipment

Questions

Emily Stuetzle
estuetzle@npcc.org

Patrick Palompo
ppalompo@npcc.org