Incident and Event Reporting

Tiffany King
Senior Auditor, WECC

Monica Vela
Cybersecurity Auditor, WECC

Saurabh Monga
Manager, Power Operations Engineering (Real-time Engineering and Energy Imbalance Market), SMUD

Josh Kretchman
Cybersecurity Emergency Operations Program Manager, SMUD

Electric Reliability & Security for the West

October 15, 2025

CIP-003-8 R2, Section 4

Responsible Entities shall include each of the sections provided below in the cyber security plan(s) required under Requirement R2.

Section 4. Cyber Security Incident Response: Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

CIP-003-8 R2, Section 4

4.1 Identification, classification, and response to Cyber Security Incidents;

4.2 Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC), unless prohibited by law;

4.3 Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals;

4.4 Incident handling for Cyber Security Incidents;

4.5 Testing the Cyber Security Incident response plan(s) at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident; and

4.6 Updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.

Definitions

Cyber Security Incident:

A malicious act or suspicious event that:

- For a high or medium impact BES Cyber System, compromises or attempts to compromise (1) an Electronic Security Perimeter, (2) a Physical Security Perimeter, or (3) an Electronic Access Control or Monitoring System; or
- Disrupts or attempts to disrupt the operation of a BES Cyber System

Reportable Cyber Security Incident:

A Cyber Security Incident that compromised or disrupted:

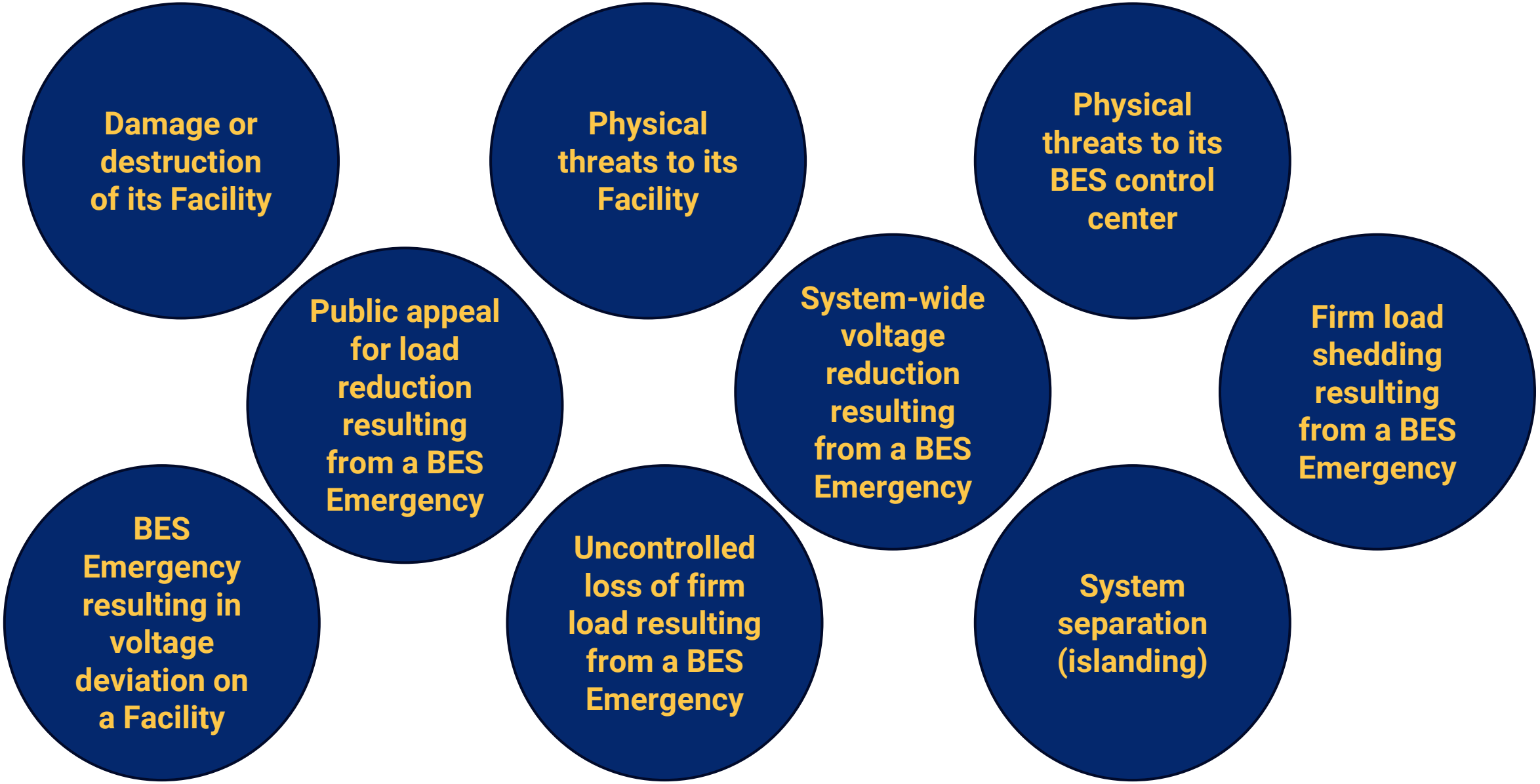
- A BES Cyber System that performs one or more reliability tasks of a functional entity;
- An Electronic Security Perimeter of a high or medium impact BES Cyber System; or
- An Electronic Access Control or Monitoring System of a high or medium impact BES Cyber System

EOP-004-4

R1. Each Responsible Entity shall have an event reporting Operating Plan in accordance with EOP-004-4 Attachment 1 that includes the protocol(s) for reporting to the Electric Reliability Organization and other organizations (e.g., the Regional Entity, company personnel, the Responsible Entity's Reliability Coordinator, law enforcement, or governmental authority).

R2. Each Responsible Entity shall report events specified in EOP-004-4 Attachment 1 to the entities specified per their event reporting Operating Plan by the later of 24 hours of recognition of meeting an event type threshold for reporting or by the end of the Responsible Entity's next business day (4 p.m. local time will be considered the end of the business day).

EOP-004-4 Attachment 1



EOP-004-4 Attachment 1

- Generation loss
- Complete loss of of-site power to a nuclear generating plant (grid supply)
- Transmission loss
- Unplanned evacuation of its BES control center
- Complete loss of Interpersonal Communication and Alternative Interpersonal Communication capability at its staffed BES control center
- Complete loss of monitoring or control capability at its staffed BES control center

Definitions

Facility:

A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer).

BES Emergency:

Any abnormal system condition that requires automatic or immediate manual action to prevent or limit the failure of transmission facilities or generation supply that could adversely affect the reliability of the Bulk Electric System.

Interpersonal Communication:

Any medium that allows two or more individuals to interact, consult, or exchange information.

Alternate Interpersonal Communication:

Any Interpersonal Communication that is able to serve as a substitute for, and does not utilize the same infrastructure (medium) as, Interpersonal Communication used for day-to-day operation.

Comparison

	CIP-003-8 R2, Section 4	EOP-004-4
Documented Plan	✓	✓
Roles & Responsibilities	✓	☐
Identify	✓	✓
Classify	✓	✓
Report	✓	✓
Respond	✓	✓
Exercises	✓	☐
Updating Plan	✓	☐

Resources

- NIST Incident Response Framework
- E-ISAC
- Controls Guidance and Compliance Failure Points
- WICF
- Senior Technical Advisors

WECC

WWW.WECC.ORG | (801) 582-0353

155 N 400 W, Salt Lake City, UT 84103, USA