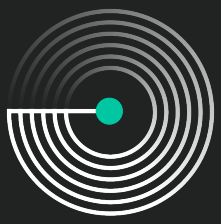

NETWORK+
SECURITY
TECHNOLOGIES

NERC CIP REFERENCE GUIDE

For when CIP gets real...

VALID THROUGH JUL 2028

TABLE OF CONTENTS

CIP-002-5.1A - BES CYBER SYSTEM CATEGORIZATION

Purpose

To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES.

Requirement R1

R1. Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3: *[Violation Risk Factor: High][Time Horizon: Operations Planning]*

- Control Centers and backup Control Centers;
- Transmission stations and substations;
- Generation resources;
- Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements;
- Special Protection Systems that support the reliable operation of the Bulk Electric System; and
- For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

1.1. Identify each of the high impact BES Cyber Systems according to Attachment 1, Section 1, if any, at each asset;

1.2. Identify each of the medium impact BES Cyber Systems according to Attachment 1, Section 2, if any, at each asset; and

1.3. Identify each asset that contains a low impact BES Cyber System according to Attachment 1, Section 3, if any (a discrete list of low impact BES Cyber Systems is not required).

M1. Acceptable evidence includes, but is not limited to, dated electronic or physical lists required by Requirement R1, and Parts 1.1 and 1.2.

Requirement R2

R2. The Responsible Entity shall: [Violation Risk Factor: Lower] [Time Horizon: Operations Planning]

2.1 Review the identifications in Requirement R1 and its parts (and update them if there are changes identified) at least once every 15 calendar months, even if it has no identified items in Requirement R1, and

2.2 Have its CIP Senior Manager or delegate approve the identifications required by Requirement R1 at least once every 15 calendar months, even if it has no identified items in Requirement R1.

M2. Acceptable evidence includes, but is not limited to, electronic or physical dated records to demonstrate that the Responsible Entity has reviewed and updated, where necessary, the identifications required in Requirement R1 and its parts, and has had its CIP Senior Manager or delegate approve the identifications required in Requirement R1 and its parts at least once every 15 calendar months, even if it has none identified in Requirement R1 and its parts, as required by Requirement R2.

Attachment 1

Impact Rating Criteria

The criteria defined in Attachment 1 do not constitute stand-alone compliance requirements, but are criteria characterizing the level of impact and are referenced by requirements.

1. High Impact Rating (H)

Each BES Cyber System used by and located at any of the following:

1.1. Each Control Center or backup Control Center used to perform the functional obligations of the Reliability Coordinator.

1.2. Each Control Center or backup Control Center used to perform the functional obligations of the Balancing Authority: 1) for generation equal to or greater than an aggregate of 3000 MW in a single Interconnection, or 2) for one or more of the assets that meet criterion 2.3, 2.6, or 2.9.

1.3. Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator for one or more of the assets that meet criterion 2.2, 2.4, 2.5, 2.7, 2.8, 2.9, or 2.10.

1.4 Each Control Center or backup Control Center used to perform the functional obligations of the Generator Operator for one or more of the assets that meet criterion 2.1, 2.3, 2.6, or 2.9.

2. Medium Impact Rating (M)

Each BES Cyber System, not included in Section 1 above, associated with any of the following:

2.1. Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of

generating units, the only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.

2.2. Each BES reactive resource or group of resources at a single location (excluding generation Facilities) with an aggregate maximum Reactive Power nameplate rating of 1000 MVAR or greater (excluding those at generation Facilities). The only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of resources that in aggregate equal or exceed 1000 MVAR.

2.3. Each generation Facility that its Planning Coordinator or Transmission Planner designates, and informs the Generator Owner or Generator Operator, as necessary to avoid an Adverse Reliability Impact in the planning horizon of more than one year.

2.4. Transmission Facilities operated at 500 kV or higher. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

2.5. Transmission Facilities that are operating between 200 kV and 499 kV at a single station or substation, where the station or substation is connected at 200 kV or higher voltages to three or more other Transmission stations or substations and has an "aggregate weighted value" exceeding 3000 according to the table below. The "aggregate weighted value" for a single station or substation is determined by summing the "weight value per line" shown in the table below for each incoming and each outgoing BES Transmission Line that is connected to another Transmission station or substation. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

Voltage Value of a Line	Weight Value per Line
Less than 200 kV (not applicable)	(not applicable)
200 kV to 299 kV	700
300 kV to 499 kV	1300
500 kV and above	0

2.6. 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.

2.7. Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.

2.8. Transmission Facilities, including generation interconnection Facilities, providing the generation interconnection required to connect generator output to the Transmission Systems that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the generation Facilities identified by any Generator Owner as a result of its application of Attachment 1, criterion 2.1 or 2.3.

2.9. Each Special Protection System (SPS), Remedial Action Scheme (RAS), or automated switching System that operates BES Elements, that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limits (IROLs) violations for failure to operate as designed or cause a reduction in one or more IROLs if destroyed, degraded, misused, or otherwise rendered unavailable.

2.10. Each system or group of Elements that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more implementing undervoltage load shedding (UVLS) or underfrequency load shedding (UFLS) under a load shedding program that is subject to one or more requirements in a NERC or regional reliability standard.

2.11. Each Control Center or backup Control Center, not already included in High Impact Rating (H) above, used to perform the functional obligations of the Generator Operator for an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection.

2.12. Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator not included in High Impact Rating (H), above.

2.13. Each Control Center or backup Control Center, not already included in High Impact Rating (H) above, used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MW in a single Interconnection.

3. Low Impact Rating (L)

BES Cyber Systems not included in Sections 1 or 2 above that are associated with any of the following assets and that meet the applicability qualifications in Section 4 - Applicability, part 4.2 – Facilities, of this standard:

3.1. Control Centers and backup Control Centers.

3.2. Transmission stations and substations.

3.3. Generation resources.

3.4. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements.

3.5. Special Protection Systems that support the reliable operation of the Bulk Electric System.

3.6. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

CIP-003-9 - SECURITY MANAGEMENT CONTROLS

Purpose
To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

Requirement R1

R1. Each Responsible Entity shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: [Violation Risk Factor: Medium] [Time Horizon: Operations Planning]

- **1.1.** For its high impact and medium impact BES Cyber Systems, if any:
  - **1.1.1.** Personnel and training (CIP-004);
  - **1.1.2.** Electronic Security Perimeters (CIP-005) including Interactive Remote Access;
  - **1.1.3.** Physical security of BES Cyber Systems (CIP-006);
  - **1.1.4.** System security management (CIP-007);
  - **1.1.5.** Incident reporting and response planning (CIP-008);
  - **1.1.6.** Recovery plans for BES Cyber Systems (CIP-009);
  - **1.1.7.** Configuration change management and vulnerability assessments (CIP-010);
  - **1.1.8.** Information protection (CIP-011); and
  - **1.1.9.** Declaring and responding to CIP Exceptional Circumstances.
- **1.2.** For its assets identified in CIP-002 containing low impact BES Cyber Systems, if any:
  - **1.2.1.** Cyber security awareness;
  - **1.2.2.** Physical security controls;
  - **1.2.3.** Electronic access controls;
  - **1.2.4.** Cyber Security Incident response;
  - **1.2.5.** Transient Cyber Assets and Removable Media malicious code risk mitigation;
  - **1.2.6.** Vendor electronic remote access security controls; and
  - **1.2.7.** Declaring and responding to CIP Exceptional Circumstances.

M1. Examples of evidence may include, but are not limited to, policy documents; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

Requirement R2

R2. Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

Note: An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required. Lists of authorized users are not required.

M2. Evidence shall include each of the documented cyber security plan(s) that collectively include each of the sections in Attachment 1 and additional evidence to demonstrate implementation of the cyber security plan(s). Additional examples of evidence per section are located in Attachment 2.

Requirement R3

R3. Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*
M3. An example of evidence may include, but is not limited to, a dated and approved document from a high level official designating the name of the individual identified as the CIP Senior Manager.

Requirement R4

R4. The Responsible Entity shall implement a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*
M4. An example of evidence may include, but is not limited to, a dated document, approved by the CIP Senior Manager, listing individuals (by name or title) who are delegated the authority to approve or authorize specifically identified items.

Attachment 1

Required Sections for Cyber Security Plan(s) for Assets Containing Low Impact BES Cyber Systems

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

Responsible Entities with multiple-impact BES Cyber Systems ratings can utilize policies, procedures, and processes for their high or medium impact BES Cyber Systems to fulfill the sections for the development of low impact cyber security plan(s). Each Responsible Entity can develop a cyber security plan(s) either by individual asset or groups of assets.

Section 1. Cyber Security Awareness: Each Responsible Entity shall reinforce, at least once every 15 calendar months, cyber security practices (which may include associated physical security practices)

Section 2. Physical Security Controls: Each Responsible Entity shall control physical access, based on need as determined by the Responsible Entity, to (1) the asset or the locations of the low impact BES Cyber Systems within the asset, and (2) the Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any.

Section 3. Electronic Access Controls: For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement electronic access controls to:

3.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that are:

- Between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s);
- Using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s); and
- Not used for time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).

3.2 Authenticate all Dial-up Connectivity, if any, that provides access to low impact BES Cyber System(s), per Cyber Asset capability.

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:

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.

Section 5. Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation: Each Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more plan(s) to achieve the objective of mitigating the risk of the introduction of malicious code to low impact BES Cyber Systems through the use of Transient Cyber Assets or Removable Media. The plan(s) shall include:

5.1 For Transient Cyber Asset(s) managed by the Responsible Entity, if any, the use of one or a combination of the following in an ongoing or on-demand manner (per Transient Cyber Asset capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

5.2 For Transient Cyber Asset(s) managed by a party other than the Responsible Entity, if any:

5.2.1 Use one or a combination of the following prior to connecting the Transient Cyber Asset to a low impact BES Cyber System (per Transient Cyber Asset capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review use of live operating system and software executable only from read-only media;
- Review of system hardening used by the party; or
- Other method(s) to mitigate the introduction of malicious code.

5.2.2 For any method used pursuant to 5.2.1, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the Transient Cyber Asset.

5.3 For Removable Media, the use of each of the following:

5.3.1 Method(s) to detect malicious code on Removable Media using a Cyber Asset other than a BES Cyber System; and

5.3.2 Mitigation of the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BES Cyber System.

Section 6. Vendor Electronic Remote Access Security Controls: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, that allow vendor electronic remote access, the Responsible Entity shall implement a process to mitigate risks associated with vendor electronic remote access, where such access has been established under Section 3.1. These processes shall include:

6.1 One or more method(s) for determining vendor electronic remote access;
6.2 One or more method(s) for disabling vendor electronic remote access; and
6.3 One or more method(s) for detecting known or suspected inbound and outbound malicious communications for vendor electronic remote access.

Attachment 2

Examples of Evidence for Cyber Security Plan(s) for Assets Containing Low Impact BES Cyber Systems

Section 1. Cyber Security Awareness: An example of evidence for Section 1 may include, but is not limited to, documentation that the reinforcement of cyber security practices occurred at least once every 15 calendar months. The evidence could be documentation through one or more of the following methods:

- Direct communications (for example, e-mails, memos, or computer-based training);
- Indirect communications (for example, posters, intranet, or brochures); or
- Management support and reinforcement (for example, presentations or meetings).

Section 2. Physical Security Controls: Examples of evidence for Section 2 may include, but are not limited to:

- Documentation of the selected access control(s) (e.g., card key, locks, perimeter controls), monitoring controls (e.g., alarm systems, human observation), or other operational, procedural, or technical physical security controls that control physical access to both:
- The asset, if any, or the locations of the low impact BES Cyber Systems within the asset; and
- The Cyber Asset(s) specified by the Responsible Entity that provide(s) electronic access controls implemented for Attachment 1, Section 3.1, if any.

Section 3. Electronic Access Controls: Examples of evidence for Section 3 may include, but are not limited to:

1. Documentation showing that at each asset or group of assets containing low impact BES Cyber Systems, routable communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset is restricted by electronic access controls to permit only inbound and outbound electronic access that the Responsible Entity deems necessary, except where an entity provides rationale that communication is used for time-sensitive protection or control functions between intelligent electronic devices. Examples of such documentation may include, but are not limited to representative diagrams that illustrate control of inbound and outbound communication(s) between the low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s) or lists of implemented electronic access controls (e.g., access control lists restricting IP addresses, ports, or services; implementing unidirectional gateways).
2. Documentation of authentication for Dial-up Connectivity (e.g., dial out only to a preprogrammed number to deliver data, dial-back modems, modems that must be remotely controlled by the control center or control room, or access control on the BES Cyber System).

Section 4. Cyber Security Incident Response: An example of evidence for Section 4 may include, but is not limited to, dated documentation, such as policies, procedures, or process documents of one or more Cyber Security Incident response plan(s) developed either by asset or group of assets that include the following processes:

1. To identify, classify, and respond to Cyber Security Incidents; to determine whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and for notifying the Electricity Information Sharing and Analysis Center (E-ISAC);
2. To identify and document the roles and responsibilities for Cyber Security Incident response by groups or individuals (e.g., initiating, documenting, monitoring, reporting, etc.);
3. For incident handling of a Cyber Security Incident (e.g., containment, eradication, or recovery/incident resolution);
4. For testing the plan(s) along with the dated documentation that a test has been completed at least once every 36 calendar months; and
5. To update, as needed, Cyber Security Incident response plan(s) within 180 calendar days after completion of a test or actual Reportable Cyber Security Incident.

Section 5. Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation:

1. Examples of evidence for Section 5.1 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.
2. Examples of evidence for Section 5.2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of live operating systems or system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.
   Examples of evidence for Attachment 1, Section 5.2.2 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigation is necessary and has been implemented prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity.
3. Examples of evidence for Section 5.3.1 may include, but are not limited to, documented process(es) of the method(s) used to detect malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Examples of evidence for Section 5.3.2 may include, but are not limited to, documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and the mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

Section 6. Vendor Electronic Remote Access Security Controls: Examples of evidence showing the implementation of the process for Section 6 may include, but are not limited to:

1. For Section 6.1, documentation showing:
   - Steps to preauthorize access;
   - Alerts generated by vendor log on;
   - Session monitoring;
   - Security information management logging alerts;
   - Time-of-need session initiation;
   - Session recording;
   - System logs; or
   - Other operational, procedural, or technical controls.
2. For Section 6.2, documentation showing:
   - Disabling vendor electronic remote access user or system accounts;
   - Disabling inbound and/or outbound hardware or software ports, services, or access permissions on applications, firewall, IDS/IPS, router, switch, VPN, Remote Desktop, remote control, or other hardware or software used for providing vendor electronic remote access;
   - Disabling communications protocols (such as IP) used for systems which establish and/or maintain vendor electronic remote access;
   - Removing physical layer connectivity (e.g., disconnect an Ethernet cable, power down equipment);
   - Administrative control documentation listing the methods, steps, or systems used to disable vendor electronic remote access; or
   - Other operational, procedural, or technical controls.
3. For Section 6.3, documentation showing implementation of processes or technologies which have the ability to detect malicious communications such as:
   - Anti-malware technologies;
   - Intrusion Detection System (IDS)/Intrusion Protection System (IPS)
   - Automated or manual log reviews;
   - Alerting; or
   - Other operational, procedural, or technical controls.

CIP-004-7 - PERSONNEL & TRAINING

Purpose
To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, security awareness, and access management in support of protecting BES Cyber Systems.

Requirement R1

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-004-7 Table R1 – Security Awareness Program. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*
M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in CIP-004-7 Table R1 – Security Awareness Program and additional evidence to demonstrate implementation as described in the Measures column of the table.

Part 1.1

Applicable Systems

- High Impact BES Cyber Systems
- Medium Impact BES Cyber Systems

Requirements
Security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems.
Measures
An example of evidence may include, but is not limited to, documentation that the quarterly reinforcement has been provided. Examples of evidence of reinforcement may include, but are not limited to, dated copies of information used to reinforce security awareness, as well as evidence of distribution, such as:

- Direct communications (for example, e-mails, memos, computer-based training); or
- Indirect communications (for example, posters, intranet, or brochures); or
- Management support and reinforcement (for example, presentations or meetings).

Requirement R2

R2. Each Responsible Entity shall implement one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in *CIP-004-7 Table R2 – Cyber Security Training Program. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*
M2. Evidence must include the training program that includes each of the applicable requirement parts in *CIP-004-7 Table R2 – Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

Part 2.1

Applicable Systems
High Impact BES Cyber Systems and their associated:

- EACMS; and
- PACS

Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:

- EACMS; and
- PACS

Requirements
Training content on:

2.1.1. Cyber security policies;
2.1.2. Physical access controls;
2.1.3. Electronic access controls;
2.1.4. The visitor control program;
2.1.5. Handling of BES Cyber System Information and its storage;
2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan;
2.1.7. Recovery plans for BES Cyber Systems;
2.1.8. Response to Cyber Security Incidents; and
2.1.9. Cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets, including Transient Cyber Assets, and with Removable Media.

Measures
Examples of evidence may include, but are not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials.

Part 2.2

Applicable Systems
High Impact BES Cyber Systems and their associated:

- EACMS; and
- PACS

Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:

- EACMS; and
- PACS

Requirements
Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to applicable Cyber Assets, except during CIP Exceptional Circumstances.
Measures
Examples of evidence may include, but are not limited to, training records and documentation of when CIP Exceptional Circumstances were invoked.

Part 2.3

Applicable Systems
High Impact BES Cyber Systems and their associated:

- EACMS; and
- PACS

Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:

- EACMS; and
- PACS

Requirements
Require completion of the training specified in Part 2.1 at least once every 15 calendar months.
Measures
Examples of evidence may include, but are not limited to, dated individual training records.

Requirement R3

R3. Each Responsible Entity shall implement one or more documented personnel risk assessment program(s) to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively include each of the applicable requirement parts in CIP-004-7 Table R3 – Personnel Risk Assessment Program. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*
M3. Evidence must include the documented personnel risk assessment programs that collectively include each of the applicable requirement parts in *CIP-004-7 Table R3 – Personnel Risk Assessment Program* and additional evidence to demonstrate implementation of the program(s).

Part 3.1

Applicable Systems
High Impact BES Cyber Systems and their associated:

- EACMS; and
- PACS

Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:

- EACMS; and
- PACS

Requirements
Process to confirm identity.
Measures
An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to confirm identity.

Part 3.2

Applicable Systems
High Impact BES Cyber Systems and their associated:

- EACMS; and
- PACS

Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:

- EACMS; and
- PACS

Requirements
Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes:

3.2.1. Current residence, regardless of duration; and

3.2.2. Other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive months or more.

If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.

Measures
An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to perform a seven year criminal history records check.

Part 3.3

Applicable Systems
High Impact BES Cyber Systems and their associated:

- EACMS; and
- PACS

Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:

- EACMS; and
- PACS

Requirements
Criteria or process to evaluate criminal history records checks for authorizing access.

Measures
An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to evaluate criminal history records checks.

Part 3.4

Applicable Systems
High Impact BES Cyber Systems and their associated:

- EACMS; and
- PACS

Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:

- EACMS; and
- PACS

Requirements
Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.
Measures
An example of evidence may include, but is not limited to, documentation of the Responsible Entity's criteria or process for verifying contractors or service vendors personnel risk assessments.

Part 3.5

Applicable Systems
High Impact BES Cyber Systems and their associated:

- EACMS; and
- PACS

Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:

- EACMS; and
- PACS

Requirements
Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 to 3.4 within the last seven years.
Measures
An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process for ensuring that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed within the last seven years.

Requirement R4

R4. Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in CIP-004-7 Table R4 – Access Management Program. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M4. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-004-7 Table R4 – Access Management Program* and additional evidence to demonstrate that the access management program was implemented as described in the Measures column of the table.

Part 4.1

Applicable Systems
High Impact BES Cyber Systems and their associated:

- EACMS; and
- PACS

Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:

- EACMS; and
- PACS

Requirements
Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances:

4.1.1. Electronic access; and
4.1.2. Unescorted physical access into a Physical Security Perimeter

Measures
An example of evidence may include, but is not limited to, dated documentation of the process to authorize electronic access, and unescorted physical access in a Physical Security Perimeter.

Part 4.2

Applicable Systems
High Impact BES Cyber Systems and their associated:

- EACMS; and
- PACS

Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:

- EACMS; and
- PACS

Requirements
Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.

Measures
Examples of evidence may include, but are not limited to:

- Dated documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of personnel who have access (i.e., user account listing), or
- Dated documentation of the verification between a list of individuals who have been authorized for access (i.e., authorization forms) and a list of individuals provisioned for access (i.e., provisioning forms or shared account listing).

Part 4.3

Applicable Systems
High Impact BES Cyber Systems and their associated:

- EACMS; and
- PACS

Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:

- EACMS; and
- PACS

Requirements
For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.
Measures
An example of evidence may include, but is not limited to, documentation of the review that includes all of the following:

1. A dated listing of all accounts/account groups or roles within the system;
2. A summary description of privileges associated with each group or role;
3. Accounts assigned to the group or role; and
4. Dated evidence showing verification of the privileges for the group are authorized and appropriate to the work function performed by people assigned to each account.

Requirement R5

R5. Each Responsible Entity shall implement one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in CIP-004-7 Table R5 – Access Revocation. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M5. Evidence must include each of the applicable documented programs that collectively include each of the applicable requirement parts in *CIP-004-7 Table R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

Part 5.1

Applicable Systems
High Impact BES Cyber Systems and their associated:

- EACMS; and
- PACS

Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:

- EACMS; and
- PACS

Requirements
A process to initiate removal of an individual's ability for unescorted physical access and Interactive Remote Access upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).
Measures
An example of evidence may include, but is not limited to, documentation of all of the following:

- Dated workflow or sign-off form verifying access removal associated with the termination action; and
- Logs or other demonstration showing such persons no longer have access.

Part 5.2

Applicable Systems
High Impact BES Cyber Systems and their associated:

- EACMS; and
- PACS

Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:

- EACMS; and
- PACS

Requirements
For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.
Measures
An example of evidence may include, but is not limited to, documentation of all of the following:

- Dated workflow or sign-off form showing a review of logical and physical access; and
- Logs or other demonstration showing such persons no longer have access that the Responsible Entity determines is not necessary.

Part 5.3

Applicable Systems
High Impact BES Cyber Systems and their associated:

- EACMS

Requirements
For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to Part 5.1) within 30 calendar days of the effective date of the termination action.
Measures
An example of evidence may include, but is not limited to, workflow or sign-off form showing access removal for any individual BES Cyber Assets and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions.

Part 5.4

Applicable Systems
High Impact BES Cyber Systems and their associated:

- EACMS

Requirements
For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access.

If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.

Measures

Examples of evidence may include, but are not limited to:

- Workflow or sign-off form showing password reset within 30 calendar days of the termination;
- Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers; or
- Documentation of the extenuating operating circumstance and workflow or sign-off form showing password reset within 10 calendar days following the end of the operating circumstance.

Requirement R6

R6. Each Responsible Entity shall implement one or more documented access management program(s) to authorize, verify, and revoke provisioned access to BCSI pertaining to the "Applicable Systems" identified in CIP-004-7 Table R6 – Access Management for BES Cyber System Information that collectively include each of the applicable requirement parts in CIP-004-7 Table R6 – Access Management for BES Cyber System Information. To be considered access to BCSI in the context of this requirement, an individual has both the ability to obtain and use BCSI. Provisioned access is to be considered the result of the specific actions taken to provide an individual(s) the means to access BCSI (e.g., may include physical keys or access cards, user accounts and associated rights and privileges, encryption keys). *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M6. Evidence must include each of the applicable documented programs that collectively include the applicable requirement parts in *CIP-004-7 Table R6 – Access Management for BES Cyber System Information* and additional evidence to demonstrate implementation as described in the Measures column of the table.

Part 6.1

Applicable Systems

High Impact BES Cyber Systems and their associated:

- EACMS; and
- PACS

Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:

- EACMS; and
- PACS

Requirements
Prior to provisioning, authorize (unless already authorized according to Part 4.1.) based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances:

6.1.1. Provisioned electronic access to electronic BCSI; and
6.1.2. Provisioned physical access to physical BCSI.

Measures
Examples of evidence may include, but are not limited to, individual records or lists that include who is authorized, the date of the authorization, and the justification of business need for the provisioned access.

Part 6.2

Applicable Systems
High Impact BES Cyber Systems and their associated:

- EACMS; and
- PACS

Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:

- EACMS; and
- PACS

Requirements
Verify at least once every 15 calendar months that all individuals with provisioned access to BCSI:

6.2.1. Have an authorization record; and
6.2.2. Still need the provisioned access to perform their current work functions, as determined by the Responsible Entity.

Measures
Examples of evidence may include, but are not limited to, the documentation of the review that includes all of the following:

- List of authorized individuals;
- List of individuals who have been provisioned access;
- Verification that provisioned access is appropriate based on need; and
- Documented reconciliation actions, if any.

Part 6.3

Applicable Systems
High Impact BES Cyber Systems and their associated:

- EACMS; and
- PACS

Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:

- EACMS; and
- PACS

Requirements
For termination actions, remove the individual's ability to use provisioned access to BCSI (unless already revoked according to Part 5.1) by the end of the next calendar day following the effective date of the termination action.

Measures
Examples of dated evidence may include, but are not limited to, access revocation records associated with the terminations and dated within the next calendar day of the termination action.

CIP-005-7 - ELECTRONIC SECURITY PERIMETER(S)

Purpose
To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

Requirement R1

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-005-7 Table R1 – Electronic Security Perimeter*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*
M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-005-7 Table R1 – Electronic Security Perimeter* and additional evidence to demonstrate implementation as described in the Measures column of the table.

Part 1.1

Applicable Systems
High Impact BES Cyber Systems and their associated:

- PCA

Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:

- PCA

Requirements
All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.
Measures
An example of evidence may include, but is not limited to, a list of all ESPs with all uniquely identifiable applicable Cyber Assets connected via a routable protocol within each ESP.

Part 1.2

Applicable Systems
High Impact BES Cyber Systems and their associated:

- PCA

Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:

- PCA

Requirements
All External Routable Connectivity must be through an identified Electronic Access Point (EAP).
Measures
An example of evidence may include, but is not limited to, network diagrams showing all external routable communication paths and the identified EAPs.

Part 1.3

Applicable Systems

- Electronic Access Points for High Impact BES Cyber Systems
- Electronic Access Points for Medium Impact BES Cyber Systems

Requirements
Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.
Measures
An example of evidence may include, but is not limited to, a list of rules (firewall, access control lists, etc.) that demonstrate that only permitted access is allowed and that each access rule has a documented reason.

Part 1.4

Applicable Systems
High Impact BES Cyber Systems with Dial-up Connectivity and their associated:

- PCA

Medium Impact BES Cyber Systems with Dial-up Connectivity and their associated:

- PCA

Requirements
Where technically feasible, perform authentication when establishing Dial-up Connectivity with applicable Cyber Assets.

Measures
An example of evidence may include, but is not limited to, a documented process that describes how the Responsible Entity is providing authenticated access through each dial-up connection.

Part 1.5

Applicable Systems

- Electronic Access Points for High Impact BES Cyber Systems
- Electronic Access Points for Medium Impact BES Cyber Systems at Control Centers

Requirements
Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.
Measures
An example of evidence may include, but is not limited to, documentation that malicious communications detection methods (e.g. intrusion detection system, application layer firewall, etc.) are implemented.

Requirement R2

R2. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts, where technically feasible, in CIP-005-7 Table R2 – Remote Access Management. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*
M2. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-7 Table R2 –Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

Part 2.1

Applicable Systems
High Impact BES Cyber Systems and their associated:

- PCA

Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:

- PCA

Requirements
For all Interactive Remote Access, utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.
Measures
Examples of evidence may include, but are not limited to, network diagrams or architecture documents.

Part 2.2

Applicable Systems
High Impact BES Cyber Systems and their associated:

- PCA

Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:

- PCA

Requirements
For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate System.
Measures
An example of evidence may include, but is not limited to, architecture documents detailing where encryption initiates and terminates.

Part 2.3

Applicable Systems
High Impact BES Cyber Systems and their associated:

- PCA

Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:

- PCA

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

Measures
An example of evidence may include, but is not limited to, architecture documents detailing the authentication factors used.
Examples of authenticators may include, but are not limited to,

- Something the individual knows such as passwords or PINs. This does not include User ID;
- Something the individual has such as tokens, digital certificates, or smart cards; or
- Something the individual is such as fingerprints, iris scans, or other biometric characteristics.

Part 2.4

Applicable Systems

High Impact BES Cyber Systems with Dial-up Connectivity and their associated:

- PCA

Medium Impact BES Cyber Systems with Dial-up Connectivity and their associated:

- PCA

Requirements
Have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access).
Measures
Examples of evidence may include, but are not limited to, documentation of the methods used to determine active vendor remote access (including Interactive Remote Access and system-to-system remote access), such as:

- Methods for accessing logged or monitoring information to determine active vendor remote access sessions;
- Methods for monitoring activity (e.g. connection tables or rule hit counters in a firewall, or user activity monitoring) or open ports (e.g. netstat or related commands to display currently active ports) to determine active system to system remote access sessions; or
- Methods that control vendor initiation of remote access such as vendors calling and requesting a second factor in order to initiate remote access.

Part 2.5

Applicable Systems
High Impact BES Cyber Systems with Dial-up Connectivity and their associated:

- PCA

Medium Impact BES Cyber Systems with Dial-up Connectivity and their associated:

- PCA

Requirements
Have one or more method(s) to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access).
Measures
Examples of evidence may include, but are not limited to, documentation of the methods(s) used to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access), such as:

- Methods to disable vendor remote access at the applicable Electronic Access Point for system-to-system remote access; or
- Methods to disable vendor Interactive Remote Access at the applicable Intermediate System.

Requirement R3

R3. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts in CIP-005-7 Table R3 –Vendor Remote Access Management for EACMS and PACS. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].
M3. Evidence must include the documented processes that collectively address each of the applicable requirement parts in CIP-005-7 Table R3 – Vendor Remote Access Management and additional evidence to demonstrate implementation as described in the Measures column of the table.

Part 3.1

Applicable Systems

- EACMS and PACS associated with High Impact BES Cyber Systems
- EACMS and PACS associated with Medium Impact BES Cyber Systems with External Routable Connectivity

Requirements
Have one or more method(s) to determine authenticated vendor-initiated remote connections.
Measures
Examples of evidence may include, but are not limited to, documentation of the methods used to determine authenticated vendor-initiated remote connections, such as:

- Methods for accessing logged or monitoring information to determine authenticated vendor-initiated remote connections.

Part 3.2

Applicable Systems

- EACMS and PACS associated with High Impact BES Cyber Systems
- EACMS and PACS associated with Medium Impact BES Cyber Systems with External Routable Connectivity

Requirements
Have one or more method(s) to terminate authenticated vendor-initiated remote connections and control the ability to reconnect.
Measures
Examples of evidence may include, but are not limited to, documentation of the methods(s) used to terminate authenticated vendor-initiated remote connections to applicable systems. Examples include terminating an active vendor-initiated shell/process/session or dropping an active vendor-initiated connection in a firewall. Methods to control the ability to reconnect, if necessary, could be: disabling an Active Directory account; disabling a security token; restricting IP addresses from vendor sources in a firewall; or physically disconnecting a network cable to prevent a reconnection.

CIP-006-6 - PHYSICAL SECURITY OF BES CYBER SYSTEMS

Purpose
To manage physical access to Bulk Electric System (BES) Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

Requirement R1

R1. Each Responsible Entity shall implement one or more documented physical security plan(s) that collectively include all of the applicable requirement parts in CIP-006-6 Table R1 – Physical Security Plan. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning and Same Day Operations].*
M1. Evidence must include each of the documented physical security plans that collectively include all of the applicable requirement parts in *CIP-006-6 Table R1 – Physical Security Plan* and additional evidence to demonstrate implementation of the plan or plans as described in the Measures column of the table.

Part 1.1

Applicable Systems
Medium Impact BES Cyber Systems without External Routable Connectivity
Physical Access Control Systems (PACS) associated with:

- High Impact BES Cyber Systems, or
- Medium Impact BES Cyber Systems with External Routable Connectivity

Requirements
Define operational or procedural controls to restrict physical access.
Measures
An example of evidence may include, but is not limited to, documentation that operational or procedural controls exist.

Part 1.2

Applicable Systems
Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:

- EACMS; and
- PCA

Requirements
Utilize at least one physical access control to allow unescorted physical access into each applicable Physical Security Perimeter to only those individuals who have authorized unescorted physical access.

Measures
An example of evidence may include, but is not limited to, language in the physical security plan that describes each Physical Security Perimeter and how unescorted physical access is controlled by one or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.

Part 1.3

Applicable Systems
High Impact BES Cyber Systems and their associated:

- EACMS; and
- PCA

Requirements
Where technically feasible, utilize two or more different physical access controls (this does not require two completely independent physical access control systems) to collectively allow unescorted physical access into Physical Security Perimeters to only those individuals who have authorized unescorted physical access.

Measures
An example of evidence may include, but is not limited to, language in the physical security plan that describes the Physical Security Perimeters and how unescorted physical access is controlled by two or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.

Part 1.4

Applicable Systems
High Impact BES Cyber Systems and their associated:

- EACMS; and
- PCA

Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:

- EACMS; and
- PCA

Requirements
Monitor for unauthorized access through a physical access point into a Physical Security Perimeter.
Measures
An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized access through a physical access point into a Physical Security Perimeter.

Part 1.5

Applicable Systems
High Impact BES Cyber Systems and their associated:

- EACMS; and
- PCA

Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:

- EACMS; and
- PCA

Requirements
Issue an alarm or alert in response to detected unauthorized access through a physical access point into a Physical Security Perimeter to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection.
Measures
An example of evidence may include, but is not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized access through a physical access control into a Physical Security Perimeter and additional evidence that the alarm or alert was issued and communicated as identified in the BES Cyber Security Incident Response Plan, such as manual or electronic alarm or alert logs, cell phone or pager logs, or other evidence that documents that the alarm or alert was generated and communicated.

Part 1.6

Applicable Systems
Physical Access Control Systems (PACS) associated with:

- High Impact BES Cyber Systems, or
- Medium Impact BES Cyber Systems with External Routable Connectivity

Requirements
Monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control System.

Measures
An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized physical access to a PACS.

Part 1.7

Applicable Systems
Physical Access Control Systems (PACS) associated with:

- High Impact BES Cyber Systems, or
- Medium Impact BES Cyber Systems with External Routable Connectivity

Requirements
Issue an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of the detection.

Measures
An example of evidence may include, but is not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized physical access to Physical Access Control Systems and additional evidence that the alarm or alerts was issued and communicated as identified in the BES Cyber Security Incident Response Plan, such as alarm or alert logs, cell phone or pager logs, or other evidence that the alarm or alert was generated and communicated.

Part 1.8

Applicable Systems
High Impact BES Cyber Systems and their associated:

- EACMS; and
- PCA

Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:

- EACMS; and
- PCA

Requirements
Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each Physical Security Perimeter, with information to identify the individual and date and time of entry.
Measures
An example of evidence may include, but is not limited to, language in the physical security plan that describes logging and recording of physical entry into each Physical Security Perimeter and additional evidence to demonstrate that this logging has been implemented, such as logs of physical access into Physical Security Perimeters that show the individual and the date and time of entry into Physical Security Perimeter.

Part 1.9

Applicable Systems
High Impact BES Cyber Systems and their associated:

- EACMS; and
- PCA

Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:

- EACMS; and
- PCA

Requirements
Retain physical access logs of entry of individuals with authorized unescorted physical access into each Physical Security Perimeter for at least ninety calendar days.
Measures
An example of evidence may include, but is not limited to, dated documentation such as logs of physical access into Physical Security Perimeters that show the date and time of entry into Physical Security Perimeter.

Part 1.10

Applicable Systems
High Impact BES Cyber Systems and their associated:

- PCA

Medium Impact BES Cyber Systems at Control Centers and their associated:

- PCA

Requirements
Restrict physical access to cabling and other nonprogrammable communication components used for connection between applicable Cyber Assets within the same Electronic Security Perimeter in those instances when such cabling and components are located outside of a Physical Security Perimeter.
Where physical access restrictions to such cabling and components are not implemented, the Responsible Entity shall document and implement one or more of the following:

- Encryption of data that transits such cabling and components; or
- Monitoring the status of the communication link composed of such cabling and components and issuing an alarm or alert in response to detected communication failures to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection; or
- An equally effective logical protection.

Measures
An example of evidence may include, but is not limited to, records of the Responsible Entity's implementation of the physical access restrictions (e.g., cabling and components secured through conduit or secured cable trays) encryption, monitoring, or equally effective logical protections.

Requirement R2

R2. Each Responsible Entity shall implement one or more documented visitor control program(s) that include each of the applicable requirement parts in CIP-006-6 Table R2 – Visitor Control Program. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]
M2. Evidence must include one or more documented visitor control programs that collectively include each of the applicable requirement parts in CIP-006-6 Table R2 – Visitor Control Program and additional evidence to demonstrate implementation as described in the Measures column of the table.

Part 2.1

Applicable Systems
High Impact BES Cyber Systems and their associated:

- EACMS; and
- PCA

Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:

- EACMS; and
- PCA

Requirements
Require continuous escorted access of visitors (individuals who are provided access but are not authorized for unescorted physical access) within each Physical Security Perimeter, except during CIP Exceptional Circumstances.
Measures
An example of evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters and additional evidence to demonstrate that the process was implemented, such as visitor logs.

Part 2.2

Applicable Systems
High Impact BES Cyber Systems and their associated:

- EACMS; and
- PCA

Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:

- EACMS; and
- PCA

Requirements
Require manual or automated logging of visitor entry into and exit from the Physical Security Perimeter that includes date and time of the initial entry and last exit, the visitor's name, and the name of an individual point of contact responsible for the visitor, except during CIP Exceptional Circumstances.
Measures
An example of evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters and additional evidence to demonstrate that the process was implemented, such as dated visitor logs that include the required information.

Part 2.3

Applicable Systems
High Impact BES Cyber Systems and their associated:

- EACMS; and
- PCA

Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:

- EACMS; and
- PCA

Requirements
Retain visitor logs for at least ninety calendar days.
Measures
An example of evidence may include, but is not limited to, documentation showing logs have been retained for at least ninety calendar days.

Requirement R3

R3. Each Responsible Entity shall implement one or more documented Physical Access Control System maintenance and testing program(s) that collectively include each of the applicable requirement parts in CIP-006-6 Table R3 – Maintenance and Testing Program. [Violation Risk Factor: Medium] [Time Horizon: Long Term Planning].
M3. Evidence must include each of the documented Physical Access Control System maintenance and testing programs that collectively include each of the applicable requirement parts in CIP-006-6 Table R3 – Maintenance and Testing Program and additional evidence to demonstrate implementation as described in the Measures column of the table.

Part 3.1

Applicable Systems
Physical Access Control Systems (PACS) associated with:

- High Impact BES Cyber Systems, or
- Medium Impact BES Cyber Systems with External Routable Connectivity

Locally mounted hardware or devices at the Physical Security Perimeter associated with:

- High Impact BES Cyber Systems, or
- Medium Impact BES Cyber Systems with External Routable Connectivity

Requirements
Maintenance and testing of each Physical Access Control System and locally mounted hardware or devices at the Physical Security Perimeter at least once every 24 calendar months to ensure they function properly.

Measures
An example of evidence may include, but is not limited to, a maintenance and testing program that provides for testing each Physical Access Control System and locally mounted hardware or devices associated with each applicable Physical Security Perimeter at least once every 24 calendar months and additional evidence to demonstrate that this testing was done, such as dated maintenance records, or other documentation showing testing and maintenance has been performed on each applicable device or system at least once every 24 calendar months.

CIP-007-6 - SYSTEMS SECURITY MANAGEMENT

Purpose
To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

Requirement R1

R1. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R1 – Ports and Services. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*
M1. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-007-6 Table R1 – Ports and Services* and additional evidence to demonstrate implementation as described in the Measures column of the table.

Part 1.1

Applicable Systems
High Impact BES Cyber Systems and their associated:

- EACMS;
- PACS; and
- PCA

Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:

- EACMS;
- PACS; and
- PCA

Requirements
Where technically feasible, enable only logical network accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed.

Measures
Examples of evidence may include, but are not limited to:

- Documentation of the need for all enabled ports on all applicable Cyber Assets and Electronic Access Points, individually or by group.
- Listings of the listening ports on the Cyber Assets, individually or by group, from either the device configuration files, command output (such as netstat), or network scans of open ports; or
- Configuration files of host-based firewalls or other device level mechanisms that only allow needed ports and deny all others.

Part 1.2

Applicable Systems
High Impact BES Cyber Systems and their associated:

- PCA; and
- Nonprogrammable communication components located inside both a PSP and an ESP.

Medium Impact BES Cyber Systems at Control Centers and their associated:

- PCA; and
- Nonprogrammable communication components located inside both a PSP and an ESP.

Requirements
Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media.
Measures
An example of evidence may include, but is not limited to, documentation showing types of protection of physical input/output ports, either logically through system configuration or physically using a port lock or signage.

Requirement R2

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R2 – Security Patch Management. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*
M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-6 Table R2 – Security Patch Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

Part 2.1

Applicable Systems
High Impact BES Cyber Systems and their associated:

- EACMS;
- PACS; and
- PCA

Medium Impact BES Cyber Systems and their associated:

- EACMS;
- PACS; and
- PCA

Requirements
A patch management process for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists.
Measures
An example of evidence may include, but is not limited to, documentation of a patch management process and documentation or lists of sources that are monitored, whether on an individual BES Cyber System or Cyber Asset basis.

Part 2.2

Applicable Systems
High Impact BES Cyber Systems and their associated:

- EACMS;
- PACS; and
- PCA

Medium Impact BES Cyber Systems and their associated:

- EACMS;
- PACS; and
- PCA

Requirements
At least once every 35 calendar days, evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1.

Measures
An example of evidence may include, but is not limited to, an evaluation conducted by, referenced by, or on behalf of a Responsible Entity of security-related patches released by the documented sources at least once every 35 calendar days.

Part 2.3

Applicable Systems
High Impact BES Cyber Systems and their associated:

- EACMS;
- PACS; and
- PCA

Medium Impact BES Cyber Systems and their associated:

- EACMS;
- PACS; and
- PCA

Requirements
For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, take one of the following actions:

- Apply the applicable patches; or
- Create a dated mitigation plan; or
- Revise an existing mitigation plan.

Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each security patch and a timeframe to complete these mitigations.

Measures
Examples of evidence may include, but are not limited to:

- Records of the installation of the patch (e.g., exports from automated patch management tools that provide installation date, verification of BES Cyber System Component software revision, or registry exports that show software has been installed); or
- A dated plan showing when and how the vulnerability will be addressed, to include documentation of the actions to be taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch and a timeframe for the completion of these mitigations.

Part 2.4

Applicable Systems
High Impact BES Cyber Systems and their associated:

- EACMS;
- PACS; and
- PCA

Medium Impact BES Cyber Systems and their associated:

- EACMS;
- PACS; and
- PCA

Requirements
For each mitigation plan created or revised in Part 2.3, implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in Part 2.3 is approved by the CIP Senior Manager or delegate.
Measures
An example of evidence may include, but is not limited to, records of implementation of mitigations.

Requirement R3

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R3 – Malicious Code Prevention. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations].*
M3. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-6 Table R3 – Malicious Code Prevention* and additional evidence to demonstrate implementation as described in the Measures column of the table.

Part 3.1

Applicable Systems
High Impact BES Cyber Systems and their associated:

- EACMS;
- PACS; and
- PCA

Medium Impact BES Cyber Systems and their associated:

- EACMS;
- PACS; and
- PCA

Requirements
Deploy method(s) to deter, detect, or prevent malicious code.
Measures
An example of evidence may include, but is not limited to, records of the Responsible Entity's performance of these processes (e.g., through traditional antivirus, system hardening, policies, etc.).

Part 3.2

Applicable Systems
High Impact BES Cyber Systems and their associated:

- EACMS;
- PACS; and
- PCA

Medium Impact BES Cyber Systems and their associated:

- EACMS;
- PACS; and
- PCA

Requirements
Mitigate the threat of detected malicious code.
Measures
Examples of evidence may include, but are not limited to:

- Records of response processes for malicious code detection
- Records of the performance of these processes when malicious code is detected.

Part 3.3

Applicable Systems
High Impact BES Cyber Systems and their associated:

- EACMS;
- PACS; and
- PCA

Medium Impact BES Cyber Systems and their associated:

- EACMS;
- PACS; and
- PCA

Requirements
For those methods identified in Part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns.
Measures
An example of evidence may include, but is not limited to, documentation showing the process used for the update of signatures or patterns.

Requirement R4

R4. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R4 – Security Event Monitoring. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Assessment.]*
M4. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-6 Table R4 – Security Event Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

Part 4.1

Applicable Systems
High Impact BES Cyber Systems and their associated:

- EACMS;
- PACS; and
- PCA

Medium Impact BES Cyber Systems and their associated:

- EACMS;
- PACS; and
- PCA

Requirements
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.

Measures
Examples of evidence may include, but are not limited to, a paper or system generated listing of event types for which the BES Cyber System is capable of detecting and, for generated events, is configured to log. This listing must include the required types of events.

Part 4.2

Applicable Systems
High Impact BES Cyber Systems and their associated:

- EACMS;
- PACS; and
- PCA

Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:

- EACMS;
- PACS; and
- PCA

Requirements
Generate alerts for security events that the Responsible Entity determines necessitates an alert, that includes, as a minimum, each of the following types of events (per Cyber Asset or BES Cyber System capability):

4.2.1. Detected malicious code from Part 4.1; and
4.2.2. Detected failure of Part 4.1 event logging.

Measures
Examples of evidence may include, but are not limited to, paper or system-generated listing of security events that the Responsible Entity determined necessitate alerts, including paper or system generated list showing how alerts are configured.

Part 4.3

Applicable Systems
High Impact BES Cyber Systems and their associated:

- EACMS;
- PACS; and
- PCA

Medium Impact BES Cyber Systems at Control Centers and their associated:

- EACMS;
- PACS; and
- PCA

Requirements
Where technically feasible, retain applicable event logs identified in Part 4.1 for at least the last 90 consecutive calendar days except under CIP Exceptional Circumstances.
Measures
Examples of evidence may include, but are not limited to, documentation of the event log retention process and paper or system generated reports showing log retention configuration set at 90 days or greater.

Part 4.4

Applicable Systems
High Impact BES Cyber Systems and their associated:

- EACMS; and
- PCA

Requirements
Review a summarization or sampling of logged events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents.
Measures
Examples of evidence may include, but are not limited to, documentation describing the review, any findings from the review (if any), and dated documentation showing the review occurred.

Requirement R5

R5. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R5 – System Access Controls. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M5. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-6 Table 5 – System Access Controls* and additional evidence to demonstrate implementation as described in the Measures column of the table.

Part 5.1

Applicable Systems
High Impact BES Cyber Systems and their associated:

- EACMS;
- PACS; and
- PCA

Medium Impact BES Cyber Systems at Control Centers and their associated:

- EACMS;
- PACS; and
- PCA

Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:

- EACMS;
- PACS; and
- PCA

Requirements
Have a method(s) to enforce authentication of interactive user access, where technically feasible.
Measures
An example of evidence may include, but is not limited to, documentation describing how access is authenticated.

Part 5.2

Applicable Systems
High Impact BES Cyber Systems and their associated:

- EACMS;
- PACS; and
- PCA

Medium Impact BES Cyber Systems and their associated:

- EACMS;
- PACS; and
- PCA

Requirements
Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).
Measures
An example of evidence may include, but is not limited to, a listing of accounts by account types showing the enabled or generic account types in use for the BES Cyber System.

Part 5.3

Applicable Systems
High Impact BES Cyber Systems and their associated:

- EACMS;
- PACS; and
- PCA

Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:

- EACMS;
- PACS; and
- PCA

Requirements
Identify individuals who have authorized access to shared accounts.
Measures
An example of evidence may include, but is not limited to, listing of shared accounts and the individuals who have authorized access to each shared account.

Part 5.4

Applicable Systems
High Impact BES Cyber Systems and their associated:

- EACMS;
- PACS; and
- PCA

Medium Impact BES Cyber Systems and their associated:

- EACMS;
- PACS; and
- PCA

Requirements
Change known default passwords, per Cyber Asset capability.
Measures
Examples of evidence may include, but are not limited to:

- Records of a procedure that passwords are changed when new devices are in production; or
- Documentation in system manuals or other vendor documents showing default vendor passwords were generated pseudo-randomly and are thereby unique to the device.

Part 5.5

Applicable Systems
High Impact BES Cyber Systems and their associated:

- EACMS;
- PACS; and
- PCA

Medium Impact BES Cyber Systems and their associated:

- EACMS;
- PACS; and
- PCA

Requirements
For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters:

5.5.1. Password length that is, at least, the lesser of eight characters or the maximum length supported by the Cyber Asset; and

5.5.2. Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Cyber Asset.

Measures
Examples of evidence may include, but are not limited to:

- System-generated reports or screen-shots of the system-enforced password parameters, including length and complexity; or
- Attestations that include a reference to the documented procedures that were followed.

Part 5.6

Applicable Systems
High Impact BES Cyber Systems and their associated:

- EACMS;
- PACS; and
- PCA

Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:

- EACMS;
- PACS; and
- PCA

Requirements
Where technically feasible, for password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months.

Measures
Examples of evidence may include, but are not limited to:

- System-generated reports or screen-shots of the system-enforced periodicity of changing passwords; or
- Attestations that include a reference to the documented procedures that were followed.

Part 5.7

Applicable Systems
High Impact BES Cyber Systems and their associated:

- EACMS;
- PACS; and
- PCA

Medium Impact BES Cyber Systems at Control Centers and their associated:

- EACMS;
- PACS; and
- PCA

Requirements
Where technically feasible, either:

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

Measures
Examples of evidence may include, but are not limited to:

- Documentation of the account-lockout parameters; or
- Rules in the alerting configuration showing how the system notified individuals after a determined number of unsuccessful login attempts.

CIP-008-6 - INCIDENT REPORTING AND RESPONSE PLANNING

Purpose
To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements.

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].*
M1. Evidence must include each of the documented plan(s) that collectively include each of the applicable requirement parts in *CIP-008-6 Table R1 – Cyber Security Incident Response Plan Specifications*.

Part 1.1

Applicable Systems
High Impact BES Cyber Systems and their associated:

- EACMS

Medium Impact BES Cyber Systems and their associated:

- EACMS

Requirements
One or more processes to identify, classify, and respond to Cyber Security Incidents.
Measures
An example of evidence may include, but is not limited to, dated documentation of Cyber Security Incident response plan(s) that include the process(es) to identify, classify, and respond to Cyber Security Incidents.

Part 1.2

Applicable Systems
High Impact BES Cyber Systems and their associated:

- EACMS

Medium Impact BES Cyber Systems and their associated:

- EACMS

Requirements
One or more processes:

1.2.1 That include criteria to evaluate and define attempts to compromise;
1.2.2 To determine if an identified Cyber Security Incident is:

- A Reportable Cyber Security Incident; or
- An attempt to compromise, as determined by applying the criteria from Part 1.2.1, one or more systems identified in the “Applicable Systems” column for this Part; and

1.2.3 To provide notification per Requirement R4.

Measures

Examples of evidence may include, but are not limited to, dated documentation of Cyber Security Incident response plan(s) that provide guidance or thresholds for determining which Cyber Security Incidents are also Reportable Cyber Security Incidents or a Cyber Security Incident that is determined to be an attempt to compromise a system identified in the “Applicable Systems” column including justification for attempt determination criteria and documented processes for notification.

Part 1.3

Applicable Systems
High Impact BES Cyber Systems and their associated:

- EACMS

Medium Impact BES Cyber Systems and their associated:

- EACMS

Requirements
The roles and responsibilities of Cyber Security Incident response groups or individuals.
Measures
An example of evidence may include, but is not limited to, dated Cyber Security Incident response process(es) or procedure(s) that define roles and responsibilities (e.g., monitoring, reporting, initiating, documenting, etc.) of Cyber Security Incident response groups or individuals.

Part 1.4

Applicable Systems
High Impact BES Cyber Systems and their associated:

- EACMS

Medium Impact BES Cyber Systems and their associated:

- EACMS

Requirements
Incident handling procedures for Cyber Security Incidents.
Measures
An example of evidence may include, but is not limited to, dated Cyber Security Incident response process(es) or procedure(s) that address incident handling (e.g., containment, eradication, recovery/incident resolution).

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].*
M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable requirement parts in *CIP-008-6 Table R2 – Cyber Security Incident Response Plan Implementation and Testing*.

Part 2.1

Applicable Systems
High Impact BES Cyber Systems and their associated:

- EACMS

Medium Impact BES Cyber Systems and their associated:

- EACMS

Requirements
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.

Measures
Examples of evidence may include, but are not limited to, dated evidence of a lessons-learned report that includes a summary of the test or a compilation of notes, logs, and communication resulting from the test. Types of exercises may include discussion or operations based exercises.

Part 2.2

Applicable Systems
High Impact BES Cyber Systems and their associated:

- EACMS

Medium Impact BES Cyber Systems and their associated:

- EACMS

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

Measures
Examples of evidence may include, but are not limited to, incident reports, logs, and notes that were kept during the incident response process, and follow-up documentation that describes deviations taken from the plan during the incident response or exercise.

Part 2.3

Applicable Systems
High Impact BES Cyber Systems and their associated:

- EACMS

Medium Impact BES Cyber Systems and their associated:

- EACMS

Requirements
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 as per the Cyber Security Incident response plan(s) under Requirement R1.

Measures
An example of evidence may include, but is not limited to, dated documentation, such as security logs, police reports, emails, response forms or checklists, forensic analysis results, restoration records, and post-incident review notes related to Reportable Cyber Security Incidents and a Cyber Security Incident that is determined to be an attempt to compromise a system identified in the "Applicable Systems" column.

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].*
M3. Evidence must include, but is not limited to, documentation that collectively demonstrates maintenance of each Cyber Security Incident response plan according to the applicable requirement parts in *CIP-008-6 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication*.

Part 3.1

Applicable Systems
High Impact BES Cyber Systems and their associated:

- EACMS

Medium Impact BES Cyber Systems and their associated:

- EACMS

Requirements
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.

Measures
An example of evidence may include, but is not limited to, all of the following:

- Dated documentation of post incident(s) review meeting notes or follow-up report showing lessons learned associated with the Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response or dated documentation stating there were no lessons learned;
- Dated and revised Cyber Security Incident response plan showing any changes based on the lessons learned; and
- Evidence of plan update distribution including, but not limited to:
    - Emails;
    - USPS or other mail service;
    - Electronic distribution system; or
    - Training sign-in sheets.

Part 3.2

Applicable Systems
High Impact BES Cyber Systems and their associated:

- EACMS

Medium Impact BES Cyber Systems and their associated:

- EACMS

Requirements
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.

Measures
An example of evidence may include, but is not limited to:

- Dated and revised Cyber Security Incident response plan with changes to the roles or responsibilities, responders or technology; and
- Evidence of plan update distribution including, but not limited to:
    - Emails;
    - USPS or other mail service;
    - Electronic distribution system; or
    - Training sign-in sheets.

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),1 or their successors, of a Reportable Cyber Security Incident and a Cyber Security Incident that was an attempt to compromise, as determined by applying the criteria from Requirement R1, Part 1.2.1, 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].*
M4. Evidence must include, but is not limited to, documentation that collectively demonstrates notification of each determined Reportable Cyber Security Incident and a Cyber Security Incident that was an attempt to compromise a system identified in the "Applicable Systems" column according to the applicable requirement parts in *CIP-008-6 Table R4 – Notifications and Reporting for Cyber Security Incidents.*

Part 4.1

Applicable Systems
High Impact BES Cyber Systems and their associated:

- EACMS

Medium Impact BES Cyber Systems and their associated:

- EACMS

Requirements
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.

Measures
Examples of evidence may include, but are not limited to, dated documentation of initial notifications and updates to the E-ISAC and NCCIC.

Part 4.2

Applicable Systems
High Impact BES Cyber Systems and their associated:

- EACMS

Medium Impact BES Cyber Systems and their associated:

- EACMS

Requirements
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.

Measures
Examples of evidence may include, but are not limited to, dated documentation of notices to the E-ISAC and NCCIC.

Part 4.3

Applicable Systems
High Impact BES Cyber Systems and their associated:

- EACMS

Medium Impact BES Cyber Systems and their associated:

- EACMS

Requirements
Provide updates, if any, within 7 calendar days of determination of new or changed attribute information required in Part 4.1.
Measures
Examples of evidence may include, but are not limited to, dated documentation of submissions to the E-ISAC and NCCIC.

CIP-009-6 - RECOVERY PLANS FOR BES CYBER SYSTEMS

Purpose
To recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES.

Requirement R1

R1. Each Responsible Entity shall have one or more documented recovery plan(s) that collectively include each of the applicable requirement parts in CIP-009-6 Table R1 – Recovery Plan Specifications. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning].*
M1. Evidence must include the documented recovery plan(s) that collectively include the applicable requirement parts in *CIP-009-6 Table R1 – Recovery Plan Specifications*.

Part 1.1

Applicable Systems
High Impact BES Cyber Systems and their associated:

- EACMS; and
- PACS

Medium Impact BES Cyber Systems and their associated:

- EACMS; and
- PACS

Requirements
Conditions for activation of the recovery plan(s).
Measures
An example of evidence may include, but is not limited to, one or more plans that include language identifying conditions for activation of the recovery plan(s).

Part 1.2

Applicable Systems
High Impact BES Cyber Systems and their associated:

- EACMS; and
- PACS

Medium Impact BES Cyber Systems and their associated:

- EACMS; and
- PACS

Requirements
Roles and responsibilities of responders.
Measures
An example of evidence may include, but is not limited to, one or more recovery plans that include language identifying the roles and responsibilities of responders.

Part 1.3

Applicable Systems
High Impact BES Cyber Systems and their associated:

- EACMS; and
- PACS

Medium Impact BES Cyber Systems and their associated:

- EACMS; and
- PACS

Requirements
One or more processes for the backup and storage of information required to recover BES Cyber System functionality.
Measures
An example of evidence may include, but is not limited to, documentation of specific processes for the backup and storage of information required to recover BES Cyber System functionality.

Part 1.4

Applicable Systems
High Impact BES Cyber Systems and their associated:

- EACMS; and
- PACS

Medium Impact BES Cyber Systems at Control Centers and their associated:

- EACMS; and
- PACS

Requirements
One or more processes to verify the successful completion of the backup processes in Part 1.3 and to address any backup failures.
Measures
An example of evidence may include, but is not limited to, logs, workflow or other documentation confirming that the backup process completed successfully and backup failures, if any, were addressed.

Part 1.5

Applicable Systems
High Impact BES Cyber Systems and their associated:

- EACMS; and
- PACS

Medium Impact BES Cyber Systems and their associated:

- EACMS; and
- PACS

Requirements
One or more processes to preserve data, per Cyber Asset capability, for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s). Data preservation should not impede or restrict recovery.
Measures
An example of evidence may include, but is not limited to, procedures to preserve data, such as preserving a corrupted drive or making a data mirror of the system before proceeding with recovery.

Requirement R2

R2. Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable requirement parts in CIP-009-6 Table R2 – Recovery Plan Implementation and Testing. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-time Operations.]*
M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable requirement parts in *CIP-009-6 Table R2 – Recovery Plan Implementation and Testing*.

Part 2.1

Applicable Systems
High Impact BES Cyber Systems and their associated:

- EACMS; and
- PACS

Medium Impact BES Cyber Systems at Control Centers and their associated:

- EACMS; and
- PACS

Requirements
Test each of the recovery plans referenced in Requirement R1 at least once every 15 calendar months:

- By recovering from an actual incident;
- With a paper drill or tabletop exercise; or
- With an operational exercise.

Measures
An example of evidence may include, but is not limited to, dated evidence of a test (by recovering from an actual incident, with a paper drill or tabletop exercise, or with an operational exercise) of the recovery plan at least once every 15 calendar months. For the paper drill or full operational exercise, evidence may include meeting notices, minutes, or other records of exercise findings.

Part 2.2

Applicable Systems
High Impact BES Cyber Systems and their associated:

- EACMS; and
- PACS

Medium Impact BES Cyber Systems at Control Centers and their associated:

- EACMS; and
- PACS

Requirements
Test a representative sample of information used to recover BES Cyber System functionality at least once every 15 calendar months to ensure that the information is useable and is compatible with current configurations.
An actual recovery that incorporates the information used to recover BES Cyber System functionality substitutes for this test.
Measures
An example of evidence may include, but is not limited to, operational logs or test results with criteria for testing the usability (e.g. sample tape load, browsing tape contents) and compatibility with current system configurations (e.g. manual or automated comparison checkpoints between backup media contents and current configuration).

Part 2.3

Applicable Systems
High Impact BES Cyber Systems
Requirements
Test each of the recovery plans referenced in Requirement R1 at least once every 36 calendar months through an operational exercise of the recovery plans in an environment representative of the production environment.
An actual recovery response may substitute for an operational exercise.
Measures
Examples of evidence may include, but are not limited to, dated documentation of:

- An operational exercise at least once every 36 calendar months between exercises, that demonstrates recovery in a representative environment; or
- An actual recovery response that occurred within the 36 calendar month timeframe that exercised the recovery plans.

Requirement R3

R3. Each Responsible Entity shall maintain each of its recovery plan(s) in accordance with each of the applicable requirement parts in *CIP-009-6 Table R3 – Recovery Plan Review, Update and Communication*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M3. Acceptable evidence includes, but is not limited to, each of the applicable requirement parts in *CIP-009-6 Table R3 – Recovery Plan Review, Update and Communication.*

Part 3.1

Applicable Systems
High Impact BES Cyber Systems and their associated:

- EACMS; and
- PACS

Medium Impact BES Cyber Systems at Control Centers and their associated:

- EACMS; and
- PACS

Requirements
No later than 90 calendar days after completion of a recovery plan test or actual recovery:

3.1.1. Document any lessons learned associated with a recovery plan test or actual recovery or document the absence of any lessons learned;

3.1.2. Update the recovery 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 recovery plan of the updates to the recovery plan based on any documented lessons learned.

Measures
An example of evidence may include, but is not limited to, all of the following:

- Dated documentation of identified deficiencies or lessons learned for each recovery plan test or actual incident recovery or dated documentation stating there were no lessons learned;
- Dated and revised recovery plan showing any changes based on the lessons learned; and
- Evidence of plan update distribution including, but not limited to:
  - Emails;
  - USPS or other mail service;
  - Electronic distribution system; or
  - Training sign-in sheets.

Part 3.2

Applicable Systems
High Impact BES Cyber Systems and their associated:

- EACMS; and
- PACS

Medium Impact BES Cyber Systems at Control Centers and their associated:

- EACMS; and
- PACS

Requirements
No later than 60 calendar days after a change to the roles or responsibilities, responders, or technology that the Responsible Entity determines would impact the ability to execute the recovery plan:

3.2.1. Update the recovery plan; and

3.2.2. Notify each person or group with a defined role in the recovery plan of the updates.

Measures
An example of evidence may include, but is not limited to, all of the following:

- Dated and revised recovery plan with changes to the roles or responsibilities, responders, or technology; and
- Evidence of plan update distribution including, but not limited to:
  - Emails;
  - USPS or other mail service;
  - Electronic distribution system; or
  - Training sign-in sheets.

CIP-010-4 - CONFIGURATION CHANGE MANAGEMENT AND VULNERABILITY ASSESSMENTS

Purpose
To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

Requirement R1

R1. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-4 Table R1 – Configuration Change Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*
M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-4 Table R1 – Configuration Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

Part 1.1

Applicable Systems
High Impact BES Cyber Systems and their associated:

- EACMS;
- PACS; and
- PCA

Medium Impact BES Cyber Systems and their associated:

- EACMS;
- PACS; and
- PCA

Requirements
Develop a baseline configuration, individually or by group, which shall include the following items:

1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists;
1.1.2. Any commercially available or open-source application software (including version) intentionally installed;
1.1.3. Any custom software installed;
1.1.4. Any logical network accessible ports; and
1.1.5. Any security patches applied.

Measures
Examples of evidence may include, but are not limited to:

- A spreadsheet identifying the required items of the baseline configuration for each Cyber Asset, individually or by group; or
- A record in an asset management system that identifies the required items of the baseline configuration for each Cyber Asset, individually or by group.

Part 1.2

Applicable Systems
High Impact BES Cyber Systems and their associated:

- EACMS;
- PACS; and
- PCA

Medium Impact BES Cyber Systems and their associated:

- EACMS;
- PACS; and
- PCA

Requirements
Authorize and document changes that deviate from the existing baseline configuration.
Measures
Examples of evidence may include, but are not limited to:

- A change request record and associated electronic authorization (performed by the individual or group with the authority to authorize the change) in a change management system for each change; or
- Documentation that the change was performed in accordance with the requirement.

Part 1.3

Applicable Systems
High Impact BES Cyber Systems and their associated:

- EACMS;
- PACS; and
- PCA

Medium Impact BES Cyber Systems and their associated:

- EACMS;
- PACS; and
- PCA

Requirements
For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.
Measures
An example of evidence may include, but is not limited to, updated baseline documentation with a date that is within 30 calendar days of the date of the completion of the change.

Part 1.4

Applicable Systems
High Impact BES Cyber Systems and their associated:

- EACMS;
- PACS; and
- PCA

Medium Impact BES Cyber Systems and their associated:

- EACMS;
- PACS; and
- PCA

Requirements
For a change that deviates from the existing baseline configuration:

1.4.1. Prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change;
1.4.2. Following the change, verify that
required cyber security controls determined in 1.4.1 are not adversely affected; and
1.4.3. Document the results of the verification.

Measures
An example of evidence may include, but is not limited to, a list of cyber security controls verified or tested along with the dated test results.

Part 1.5

Applicable Systems
High Impact BES Cyber Systems
Requirements
Where technically feasible, for each change that deviates from the existing baseline configuration:

1.5.1. Prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and

1.5.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.

Measures
An example of evidence may include, but is not limited to, a list of cyber security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including the date of the test.

Part 1.6

Applicable Systems
High Impact BES Cyber Systems and their associated:

- EACMS; and
- PACS

Medium Impact BES Cyber Systems and their associated:

- EACMS; and
- PACS

Note: Implementation does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Part 1.6: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.

Requirements

Prior to a change that deviates from the existing baseline configuration associated with baseline items in Parts 1.1.1, 1.1.2, and 1.1.5, and when the method to do so is available to the Responsible Entity from the software source:

1.6.1. Verify the identity of the software source; and

1.6.2. Verify the integrity of the software obtained from the software source.

Measures

An example of evidence may include, but is not limited to a change request record that demonstrates the verification of identity of the software source and integrity of the software was performed prior to the baseline change or a process which documents the mechanisms in place that would automatically ensure the identity of the software source and integrity of the software.

Requirement R2

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-4 Table R2 – Configuration Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-4 Table R2 – Configuration Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

Part 2.1

Applicable Systems

High Impact BES Cyber Systems and their associated:

- EACMS; and
- PCA

Requirements

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.

Measures
An example of evidence may include, but is not limited to, logs from a system that is monitoring the configuration along with records of investigation for any unauthorized changes that were detected.

Requirement R3

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-010-3 Table R3– Vulnerability Assessments. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*
M3. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-3 Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

Part 3.1

Applicable Systems
High Impact BES Cyber Systems and their associated:

- EACMS;
- PACS; and
- PCA

Medium Impact BES Cyber Systems and their associated:

- EACMS;
- PACS; and
- PCA

Requirements
At least once every 15 calendar months, conduct a paper or active vulnerability assessment.
Measures
Examples of evidence may include, but are not limited to:

- A document listing the date of the assessment (performed at least once every 15 calendar months), the controls assessed for each BES Cyber System along with the method of assessment; or
- A document listing the date of the assessment and the output of any tools used to perform the assessment.

Part 3.2

Applicable Systems
High Impact BES Cyber Systems
Requirements
Where technically feasible, at least once every 36 calendar months:

3.2.1. Perform an active vulnerability assessment in a test environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration of the BES Cyber System in a production environment; and

3.2.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.

Measures
An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed at least once every 36 calendar months), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment.

Part 3.3

Applicable Systems
High Impact BES Cyber Systems and their associated:

- EACMS; and
- PCA

Requirements
Prior to adding a new applicable Cyber Asset to a production environment, perform an active vulnerability assessment of the new Cyber Asset, except for CIP Exceptional Circumstances and like replacements of the same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing Cyber Asset.
Measures
An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed prior to the commissioning of the new Cyber Asset) and the output of any tools used to perform the assessment.

Part 3.4

Applicable Systems
High Impact BES Cyber Systems and their associated:

- EACMS;
- PACS; and
- PCA

Medium Impact BES Cyber Systems and their associated:

- EACMS;
- PACS; and
- PCA

Requirements
Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.
Measures
An example of evidence may include, but is not limited to, a document listing the results or the review or assessment, a list of action items, documented proposed dates of completion for the action plan, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items).

Requirement R4

R4. Each Responsible Entity, for its high impact and medium impact BES Cyber Systems and associated Protected Cyber Assets, shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) for Transient Cyber Assets and Removable Media that include the sections in Attachment 1. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*
M4. Evidence shall include each of the documented plan(s) for Transient Cyber Assets and Removable Media that collectively include each of the applicable sections in Attachment 1 and additional evidence to demonstrate implementation of plan(s) for Transient Cyber Assets and Removable Media. Additional examples of evidence per section are located in Attachment 2. If a Responsible Entity does not use Transient Cyber Asset(s) or Removable Media, examples of evidence include, but are not limited to, a statement, policy, or other document that states the Responsible Entity does not use Transient Cyber Asset(s) or Removable Media.

Attachment 1

Required Sections for Plans for Transient Cyber Assets and Removable Media

Responsible Entities shall include each of the sections provided below in their plan(s) for Transient Cyber Assets and Removable Media as required under Requirement R4.

Section 1. Transient Cyber Asset(s) Managed by the Responsible Entity.

1.1. Transient Cyber Asset Management: Responsible Entities shall manage Transient Cyber Asset(s), individually or by group: (1) in an ongoing manner to ensure compliance with applicable requirements at all times, (2) in an on-demand manner applying the applicable requirements before connection to a BES Cyber System, or (3) a combination of both (1) and (2) above.

1.2. Transient Cyber Asset Authorization: For each individual or group of Transient Cyber Asset(s), each Responsible Entity shall authorize:

1.2.1. Users, either individually or by group or role;

1.2.2. Locations, either individually or by group; and

1.2.3. Uses, which shall be limited to what is necessary to perform business functions.

1.3. Software Vulnerability Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the Transient Cyber Asset (per Transient Cyber Asset capability):

- Security patching, including manual or managed updates;
- Live operating system and software executable only from read-only media;
- System hardening; or
- Other method(s) to mitigate software vulnerabilities.

1.4. Introduction of Malicious Code Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the introduction of malicious code (per Transient Cyber Asset capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

1.5. Unauthorized Use Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of unauthorized use of Transient Cyber Asset(s):

- Restrict physical access;
- Full-disk encryption with authentication;
- Multi-factor authentication; or
- Other method(s) to mitigate the risk of unauthorized use.

Section 2. Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity.

2.1. Software Vulnerabilities Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the Transient Cyber Asset (per Transient Cyber Asset capability):

- Review of installed security patch(es);
- Review of security patching process used by the party;
- Review of other vulnerability mitigation performed by the party; or
- Other method(s) to mitigate software vulnerabilities.

2.2. Introduction of malicious code mitigation: Use one or a combination of the following methods to achieve the objective of mitigating malicious code (per Transient Cyber Asset capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review use of live operating system and software executable only from read-only media;
- Review of system hardening used by the party; or
- Other method(s) to mitigate malicious code.

2.3. For any method used to mitigate software vulnerabilities or malicious code as specified in 2.1 and 2.2, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the Transient Cyber Asset.

Section 3. Removable Media

3.1. Removable Media Authorization: For each individual or group of Removable Media, each Responsible Entity shall authorize:

3.1.1. Users, either individually or by group or role; and

3.1.2. Locations, either individually or by group.

3.2. Malicious Code Mitigation: To achieve the objective of mitigating the threat of introducing malicious code to high impact or medium impact BES Cyber Systems and their associated Protected Cyber Assets, each Responsible Entity shall:

3.2.1. Use method(s) to detect malicious code on Removable Media using a Cyber Asset other than a BES Cyber System or Protected Cyber Assets; and

3.2.2. Mitigate the threat of detected malicious code on Removable Media prior to connecting the Removable Media to a high impact or medium impact BES Cyber System or associated Protected Cyber Assets.

Attachment 2

Examples of Evidence for Plans for Transient Cyber Assets and Removable Media

Section 1.1: Examples of evidence for Section 1.1 may include, but are not limited to, the method(s) of management for the Transient Cyber Asset(s). This can be included as part of the Transient Cyber Asset plan(s), part of the documentation related to authorization of Transient Cyber Asset(s) managed by the Responsible Entity or part of a security policy.

Section 1.2: Examples of evidence for Section 1.2 may include, but are not limited to, documentation from asset management systems, human resource management systems, or forms or spreadsheets that show authorization of Transient Cyber Asset(s) managed by the Responsible Entity. Alternatively, this can be documented in the overarching plan document.

Section 1.3: Examples of evidence for Section 1.3 may include, but are not limited to, documentation of the method(s) used to mitigate software vulnerabilities posed by unpatched software such as security patch management implementation, the use of live operating systems from read-only media, system hardening practices or other method(s) to mitigate the software vulnerability posed by unpatched software. Evidence can be from change management systems, automated patch management solutions, procedures or processes associated with using live operating systems, or procedures or processes associated with system hardening practices. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 1.4: Examples of evidence for Section 1.4 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 1.5: Examples of evidence for Section 1.5 may include, but are not limited to, documentation through policies or procedures of the method(s) to restrict physical access; method(s) of the full-disk encryption solution along with the authentication protocol; method(s) of the multi-factor authentication solution; or documentation of other method(s) to mitigate the risk of unauthorized use.

Section 2.1: Examples of evidence for Section 2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of installed security patch(es); memoranda, electronicmail, policies or contracts from parties other than the Responsible Entity that identify the security patching process or vulnerability mitigation performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail, system documentation or contracts that identifies acceptance by the Responsible Entity that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate software vulnerabilities for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 2.2: Examples of evidence for Section 2.2 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of live of operating systems or system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 2.3: Examples of evidence for Section 2.3 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigations are necessary and that they have been implemented prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity.

Section 3.1: Examples of evidence for Section 3.1 may include, but are not limited to, documentation from asset management systems, human resource management systems, forms or spreadsheets that shows authorization of Removable Media. The documentation must identify Removable Media, individually or by group of Removable Media, along with the authorized users, either individually or by group or role, and the authorized locations, either individually or by group.

Section 3.2: Examples of evidence for Section 3.2 may include, but are not limited to, documented process(es) of the method(s) used to mitigate malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and that show mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

CIP-011-3 - INFORMATION PROTECTION

Purpose
To prevent unauthorized access to BES Cyber System Information (BCSI) by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

Requirement R1

R1. Each Responsible Entity shall implement one or more documented information protection program(s) for BES Cyber System Information (BCSI) pertaining to "Applicable Systems" identified in *CIP-011-3 Table R1 – Information Protection Program* that collectively includes each of the applicable requirement parts in *CIP-011-3 Table R1 – Information Protection Program. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*
M1. Evidence for the information protection program must include the applicable requirement parts in *CIP-011-3 Table R1 – Information Protection Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

Part 1.1

Applicable Systems
High Impact BES Cyber Systems and their associated:

- EACMS; and
- PACS

Medium Impact BES Cyber Systems and their associated:

- EACMS; and
- PACS

Requirements
Method(s) to identify BCSI.

Measures
Examples of acceptable evidence may include, but are not limited to, the following:

- Documented method(s) to identify BCSI from the entity's information protection program; or
- Indications on information (e.g., labels or classification) that identify BCSI as designated in the entity's information protection program; or
- Training materials that provide personnel with sufficient knowledge to identify BCSI; or
- Storage locations identified for housing BCSI in the entity's information protection program.

Part 1.2

Applicable Systems
High Impact BES Cyber Systems and their associated:

- EACMS; and
- PACS

Medium Impact BES Cyber Systems and their associated:

- EACMS; and
- PACS

Requirements
Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality.
Measures
Examples of evidence for on-premise BCSI may include, but are not limited to, the following:

- Procedures for protecting and securely handling, which include topics such as storage, security during transit, and use of BCSI; or
- Records indicating that BCSI is handled in a manner consistent with the entity's documented procedure(s).

Examples of evidence for off-premise BCSI may include, but are not limited to, the following:

- Implementation of electronic technical method(s) to protect electronic BCSI (e.g., data masking, encryption, hashing, tokenization, cipher, electronic key management); or
- Implementation of physical technical method(s) to protect physical BCSI (e.g., physical lock and key management, physical badge management, biometrics, alarm system); or
- Implementation of administrative method(s) to protect BCSI (e.g., vendor service risk assessments, business agreements).

Requirement R2

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include the applicable requirement parts in *CIP-011-3 Table R2 – BES Cyber Asset Reuse and Disposal*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning].*
M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-011-3 Table R2 – BES Cyber Asset Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

Part 2.1

Applicable Systems
High Impact BES Cyber Systems and their associated:

- EACMS;
- PACS; and
- PCA

Medium Impact BES Cyber Systems and their associated:

- EACMS;
- PACS; and
- PCA

Requirements
Prior to the release for reuse of applicable Cyber Assets that contain BCSI (except for reuse within other systems identified in the “Applicable Systems” column), the Responsible Entity shall take action to prevent the unauthorized retrieval of BCSI from the Cyber Asset data storage media.
Measures
Examples of acceptable evidence may include, but are not limited to, the following:

- Records tracking sanitization actions taken to prevent unauthorized retrieval of BCSI such as clearing, purging, or destroying; or
- Records tracking actions such as encrypting, retaining in the Physical Security Perimeter or other methods used to prevent unauthorized retrieval of BCSI.

Part 2.2

Applicable Systems
High Impact BES Cyber Systems and their associated:

- EACMS;
- PACS; and
- PCA

Medium Impact BES Cyber Systems and their associated:

- EACMS;
- PACS; and
- PCA

Requirements
Prior to the disposal of applicable Cyber Assets that contain BCSI, the Responsible Entity shall take action to prevent the unauthorized retrieval of BCSI from the Cyber Asset or destroy the data storage media.

Measures
Examples of acceptable evidence may include, but are not limited to, the following:

- Records that indicate that data storage media was destroyed prior to the disposal of an applicable Cyber Asset; or
- Records of actions taken to prevent unauthorized retrieval of BCSI prior to the disposal of an applicable Cyber Asset.

CIP-012-2 - COMMUNICATIONS BETWEEN CONTROL CENTERS

Purpose

To protect the confidentiality, integrity, and availability of Real-time Assessment and Real-time monitoring data transmitted between Control Centers.

Applicability

4.1. Functional Entities: The requirements in this standard apply to the following functional entities, referred to as "Responsible Entities," that own or operate a Control Center.

- **4.1.1.** Balancing Authority
- **4.1.2.** Generator Operator
- **4.1.3.** Generator Owner
- **4.1.4.** Reliability Coordinator
- **4.1.5.** Transmission Operator
- **4.1.6.** Transmission Owner

4.2. Exemptions: The following are exempt from Reliability Standard CIP-012-1:

- **4.2.1.** Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.
- **4.2.2.** The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.
- **4.2.3.** A Control Center that transmits to another Control Center Real-time Assessment or Real-time monitoring data pertaining only to the generation resource or Transmission station or substation co-located with the transmitting Control Center.

Requirement R1

R1. The Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) to mitigate the risks posed by unauthorized disclosure, unauthorized modification, and loss of availability, of data used in Real-time Assessment and Real-time monitoring while such data is being transmitted between any applicable Control Centers. The Responsible Entity is not required to include oral communications in its plan. The plan shall include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

- **1.1.** Identification of method(s) used to mitigate the risk(s) posed by unauthorized disclosure and unauthorized modification of data used in Real-time Assessment and Real-time monitoring while such data is being transmitted between Control Centers;
- **1.2.** Identification of method(s) used to mitigate the risk(s) posed by the loss of the ability to communicate Real-time Assessment and Real-time monitoring data between Control Centers;
- **1.3.** Identification of method(s) used to initiate the recovery of communication links used to transmit Real-time Assessment and Real-time monitoring data between Control Centers;

1.4. Identification of where the Responsible Entity implemented method(s) as required in Parts 1.1 and 1.2; and

1.5. If the Control Centers are owned or operated by different Responsible Entities, identification of the responsibilities of each Responsible Entity for implementing method(s) as required in Parts 1.1, 1.2, and 1.3.

M1. Examples of evidence may include, but are not limited to, documented plan(s) that meet the mitigation objective of Requirement R1 and documentation demonstrating the implementation of the plan(s). Examples of methods identified in the plan(s) may include, but are not limited to, one or more of the following for each Part:

Part 1.1

- Methods of mitigation used to protect against the unauthorized disclosure and unauthorized modification of the data (e.g., data masking, encryption/decryption) while such data is being transmitted between Control Centers
- Physical access restrictions to unencrypted portions of the network

Part 1.2

- Identification of alternative communication paths or methods between Control Centers
- Procedures explaining the use of alternative systems or methods for providing for the availability of the data
- Service level agreements with carriers containing high availability provisions
- Availability or uptime reports for equipment supporting the transmission of Real-time Assessment and Real-time monitoring data

Part 1.3

- Contract, memorandum of understanding, meeting minutes, agreement or other information outlining the methods used for recovery
- Methods for the recovery of links such as standard operating procedures, applicable sections of CIP-009 recovery plan(s), or similar technical recovery plans
- Documentation of the process to restore assets and systems that provide communications
- Process or procedure to contact a communications link vendor to initiate and or verify restoration of service

Part 1.4

- Descriptions or logical diagrams indicating where the implemented methods reside
- Identification of points within the infrastructure where the implemented methods reside
- Third party Agreements detailing where the methods are implemented if such methods are implemented by the third party

Part 1.5

- Contract, memorandum of understanding, meeting minutes, agreement, or other documentation outlining the responsibilities of each entity

CIP-013-2 - SUPPLY CHAIN RISK MANAGEMENT

Purpose

To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems.

Applicability

4.1. Functional Entities: The requirements in this standard apply to the following functional entities, referred to as "Responsible Entities," **that own or operate a Control Center.**

- **4.1.1.** Balancing Authority
- **4.1.2.** Generator Operator
- **4.1.3.** Generator Owner
- **4.1.4.** Reliability Coordinator
- **4.1.5.** Transmission Operator
- **4.1.6.** Transmission Owner

4.2. Exemptions: The following are exempt from Reliability Standard CIP-012-1:

- **4.2.1.** Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.
- **4.2.2.** The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.
- **4.2.3.** A Control Center that transmits to another Control Center Real-time Assessment or Real-time monitoring data pertaining only to the generation resource or Transmission station or substation co-located with the transmitting Control Center.

Requirement R1

R1. Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems and their associated Electronic Access Control or Monitoring Systems (EACMS) and Physical Access Control Systems (PACS). The plan(s) shall include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. One or more process(es) used in planning for the procurement of BES Cyber Systems and their associated EACMS and PACS to identify and assess cyber security risk(s) to the Bulk Electric System from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s).

1.2. One or more process(es) used in procuring BES Cyber Systems, and their associated EACMS and PACS, that address the following, as applicable:

1.2.1. Notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;

1.2.2. Coordination of responses to vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;

1.2.3. Notification by vendors when remote or onsite access should no longer be granted to vendor representatives;

1.2.4. Disclosure by vendors of known vulnerabilities related to the products or services provided to the Responsible Entity;

1.2.5. Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES Cyber System and their associated EACMS and PACS; and

1.2.6. Coordination of controls for vendor-initiated remote access.

M1. Evidence shall include one or more documented supply chain cyber security risk management plan(s) as specified in the Requirement.

Requirement R2

R2. Each Responsible Entity shall implement its supply chain cyber security risk management plan(s) specified in Requirement R1. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

Note: Implementation of the plan does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Requirement R2: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.

M2. Evidence shall include documentation to demonstrate implementation of the supply chain cyber security risk management plan(s), which could include, but is not limited to, correspondence, policy documents, or working documents that demonstrate use of the supply chain cyber security risk management plan.

Requirement R3

R3. Each Responsible Entity shall review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. Evidence shall include the dated supply chain cyber security risk management plan(s) approved by the CIP Senior Manager or delegate(s) and additional evidence to demonstrate review of the supply chain cyber security risk management plan(s). Evidence may include, but is not limited to, policy documents, revision history, records of review, or workflow evidence from a document management system that indicate review of supply chain risk management plan(s) at least once every 15 calendar months; and documented approval by the CIP Senior Manager or delegate.

CIP-014-1 - PHYSICAL SECURITY

Purpose

To identify and protect Transmission stations and Transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in instability, uncontrolled separation, or Cascading within an Interconnection.

Applicability

4.1. Functional Entities:

4.1.1 Transmission Owner that owns a Transmission station or Transmission substation that meets any of the following criteria:

4.1.1.1 Transmission Facilities operated at 500 kV or higher. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

4.1.1.2 Transmission Facilities that are operating between 200 kV and 499 kV at a single station or substation, where the station or substation is connected at 200 kV or higher voltages to three or more other Transmission stations or substations and has an "aggregate weighted value" exceeding 3000 according to the table below. The "aggregate weighted value" for a single station or substation is determined by summing the "weight value per line" shown in the table below for each incoming and each outgoing BES Transmission Line that is connected to another Transmission station or substation. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

Voltage Value of a Line	Weight Value per Line
Less than 200 kV (not applicable)	(not applicable)
200 kV to 299 kV	700
300 kV to 499 kV	1300
500 kV and above	0

4.1.1.3 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.

4.1.1.4 Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.

4.1.2 Transmission Operator.

Exemption: Facilities in a “protected area,” as defined in 10 C.F.R. § 73.2, within the scope of a security plan approved or accepted by the Nuclear Regulatory Commission are not subject to this Standard; or, Facilities within the scope of a security plan approved or accepted by the Canadian Nuclear Safety Commission are not subject to this Standard.

Requirement R1

R1. Each Transmission Owner shall perform an initial risk assessment and subsequent risk assessments of its Transmission stations and Transmission substations (existing and planned to be in service within 24 months) that meet the criteria specified in Applicability Section 4.1.1. The initial and subsequent risk assessments shall consist of a transmission analysis or transmission analyses designed to identify the Transmission station(s) and Transmission substation(s) that if rendered inoperable or damaged could result in instability, uncontrolled separation, or Cascading within an Interconnection. *[VRF: High; Time-Horizon: Long-term Planning]*

1.1 Subsequent risk assessments shall be performed:

- At least once every 30 calendar months for a Transmission Owner that has identified in its previous risk assessment (as verified according to Requirement R2) one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could result in instability, uncontrolled separation, or Cascading within an Interconnection; or
- At least once every 60 calendar months for a Transmission Owner that has not identified in its previous risk assessment (as verified according to Requirement R2) any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in instability, uncontrolled separation, or Cascading within an Interconnection.

1.2. The Transmission Owner shall identify the primary control center that operationally controls each Transmission station or Transmission substation identified in the Requirement R1 risk assessment.

M1. Examples of acceptable evidence may include, but are not limited to, dated written or electronic documentation of the risk assessment of its Transmission stations and Transmission substations (existing and planned to be in service within 24 months) that meet the criteria in Applicability Section 4.1.1 as specified in Requirement R1. Additionally, examples of acceptable evidence may include, but are not limited to, dated written or electronic documentation of the identification of the primary control center that operationally controls each Transmission station or Transmission substation identified in the Requirement R1 risk assessment as specified in Requirement R1, Part 1.2.

Requirement R2

R2. Each Transmission Owner shall have an unaffiliated third party verify the risk assessment performed under Requirement R1. The verification may occur concurrent with or after the risk assessment performed under Requirement R1. *[VRF: Medium; Time-Horizon: Long-term Planning]*

2.1. Each Transmission Owner shall select an unaffiliated verifying entity that is either:

- A registered Planning Coordinator, Transmission Planner, or Reliability Coordinator; or
- An entity that has transmission planning or analysis experience

2.2. The unaffiliated third party verification shall verify the Transmission Owner's risk assessment performed under Requirement R1, which may include recommendations for the addition or deletion of a Transmission station(s) or Transmission substation(s). The Transmission Owner shall ensure the verification is completed within 90 calendar days following the completion of the Requirement R1 risk assessment.

2.3. If the unaffiliated verifying entity recommends that the Transmission Owner add a Transmission station(s) or Transmission substation(s) to, or remove a Transmission station(s) or Transmission substation(s) from, its identification under Requirement R1, the Transmission Owner shall either, within 60 calendar days of completion of the verification, for each recommended addition or removal of a Transmission station or Transmission substation:

- Modify its identification under Requirement R1 consistent with the recommendation; or
- Document the technical basis for not modifying the identification in accordance with the recommendation.

2.4. Each Transmission Owner shall implement procedures, such as the use of non-disclosure agreements, for protecting sensitive or confidential information made available to the unaffiliated third party verifier and to protect or exempt sensitive or confidential information developed pursuant to this Reliability Standard from public disclosure.

M2. Examples of acceptable evidence may include, but are not limited to, dated written or electronic documentation that the Transmission Owner completed an unaffiliated third party verification of the Requirement R1 risk assessment and satisfied all of the applicable provisions of Requirement R2, including, if applicable, documenting the technical basis for not modifying the Requirement R1 identification as specified under Part 2.3. Additionally, examples of evidence may include, but are not limited to, written or electronic documentation of procedures to protect information under Part 2.4.

Requirement R3

R3. For a primary control center(s) identified by the Transmission Owner according to Requirement R1, Part 1.2 that a) operationally controls an identified Transmission station or Transmission substation verified according to Requirement R2, and b) is not under the operational control of the Transmission Owner: the Transmission Owner shall, within seven calendar days following completion of Requirement R2, notify the Transmission Operator that has operational

control of the primary control center of such identification and the date of completion of Requirement R2. *[VRF: Lower; Time-Horizon: Long-term Planning]*

3.1. If a Transmission station or Transmission substation previously identified under Requirement R1 and verified according to Requirement R2 is removed from the identification during a subsequent risk assessment performed according to Requirement R1 or a verification according to Requirement R2, then the Transmission Owner shall, within seven calendar days following the verification or the subsequent risk assessment, notify the Transmission Operator that has operational control of the primary control center of the removal.

M3. Examples of acceptable evidence may include, but are not limited to, dated written or electronic notifications or communications that the Transmission Owner notified each Transmission Operator, as applicable, according to Requirement R3.

Requirement R4

R4. Each Transmission Owner that identified a Transmission station, Transmission substation, or a primary control center in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3, shall conduct an evaluation of the potential threats and vulnerabilities of a physical attack to each of their respective Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2. The evaluation shall consider the following: *[VRF: Medium; Time-Horizon: Operations Planning, Long-term Planning]*

4.1. Unique characteristics of the identified and verified Transmission station(s), Transmission substation(s), and primary control center(s);

4.2. Prior history of attack on similar facilities taking into account the frequency, geographic proximity, and severity of past physical security related events; and

4.3. Intelligence or threat warnings received from sources such as law enforcement, the Electric Reliability Organization (ERO), the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), U.S. federal and/or Canadian governmental agencies, or their successors.

M4. Examples of evidence may include, but are not limited to, dated written or electronic documentation that the Transmission Owner or Transmission Operator conducted an evaluation of the potential threats and vulnerabilities of a physical attack to their respective Transmission station(s), Transmission substation(s) and primary control center(s) as specified in Requirement R4.

Requirement R5

R5. Each Transmission Owner that identified a Transmission station, Transmission substation, or primary control center in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3, shall develop and implement a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary control center(s). The physical security plan(s) shall be

5.1. Resiliency or security measures designed collectively to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities identified during the evaluation conducted in Requirement R4.

developed within 120 calendar days following the completion of Requirement R2 and executed according to the timeline specified in the physical security plan(s). The physical security plan(s) shall include the following attributes: *[VRF: High; Time-Horizon: Long-term Planning]*

5.2. Law enforcement contact and coordination information.

5.3. A timeline for executing the physical security enhancements and modifications specified in the physical security plan.

5.4. Provisions to evaluate evolving physical threats, and their corresponding security measures, to the Transmission station(s), Transmission substation(s), or primary control center(s).

M5. Examples of evidence may include, but are not limited to, dated written or electronic documentation of its physical security plan(s) that covers their respective identified and verified Transmission station(s), Transmission substation(s), and primary control center(s) as specified in Requirement R5, and additional evidence demonstrating execution of the physical security plan according to the timeline specified in the physical security plan.

Requirement R6

R6. Each Transmission Owner that identified a Transmission station, Transmission substation, or primary control center in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3, shall have an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5. The review may occur concurrently with or after completion of the evaluation performed under Requirement R4 and the security plan development under Requirement R5. *[VRF: Medium; Time-Horizon: Long-term Planning]*

6.1. Each Transmission Owner and Transmission Operator shall select an unaffiliated third party reviewer from the following:

- An entity or organization with electric industry physical security experience and whose review staff has at least one member who holds either a Certified Protection Professional (CPP) or Physical Security Professional (PSP) certification.
- An entity or organization approved by the ERO.
- A governmental agency with physical security expertise.
- An entity or organization with demonstrated law enforcement, government, or military physical security expertise.

6.2. The Transmission Owner or Transmission Operator, respectively, shall ensure that the unaffiliated third party review is completed within 90 calendar days of completing the security plan(s) developed in Requirement R5. The unaffiliated third party review may, but is not required to, include recommended changes to the evaluation performed under Requirement R4 or the security plan(s) developed under Requirement R5.

6.3. If the unaffiliated third party reviewer recommends changes to the evaluation performed under Requirement R4 or security plan(s) developed under Requirement R5, the Transmission Owner or Transmission Operator shall, within 60 calendar days of the completion of the unaffiliated third party review, for each recommendation:

- Modify its evaluation or security plan(s) consistent with the recommendation; or
- Document the reason(s) for not modifying the evaluation or security plan(s) consistent with the recommendation.

6.4. Each Transmission Owner and Transmission Operator shall implement procedures, such as the use of non-disclosure agreements, for protecting sensitive or confidential information made available to the unaffiliated third party reviewer and to protect or exempt sensitive or confidential information developed pursuant to this Reliability Standard from public disclosure.

M6. Examples of evidence may include, but are not limited to, written or electronic documentation that the Transmission Owner or Transmission Operator had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 as specified in Requirement R6 including, if applicable, documenting the reasons for not modifying the evaluation or security plan(s) in accordance with a recommendation under Part 6.3. Additionally, examples of evidence may include, but are not limited to, written or electronic documentation of procedures to protect information under Part 6.4.

FUTURE STANDARDS

The following Standards have been approved by FERC and will become effective on the following dates:

Standard	Effective Date
CIP-002-8	07/01/2028
CIP-003-10	07/01/2028
CIP-004-8	07/01/2028
CIP-005-8	07/01/2028
CIP-006-7.1	07/01/2028
CIP-007-7.1	07/01/2028
CIP-008-7.1	07/01/2028
CIP-009-7.1	07/01/2028
CIP-010-5	07/01/2028
CIP-011-4.1	07/01/2028
CIP-013-3	07/01/2028
CIP-015-1	10/01/2028
CIP-003-11	07/01/2029

Note: Until the respective dates listed above, your organization is expected to comply with the currently effective versions of the Standards, unless otherwise approved by your Regional Entity.

CONTACT US

Questions about NERC CIP? Reach out to us individually or at info@nst.us

Matt Schwartz
Director of Sales and Marketing
(845) 405-1816
mschwartz@nst.us

Patrick Tierney
Sales Representative
(952) 290-0041
ptierney@nst.us

NETWORK + SECURITY TECHNOLOGIES

CIP HAPPENS