A. Introduction

1. **Title:** Cyber Security — Security Management Controls

2. **Number:** CIP-003-11

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

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3. Generator Operator

   4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-003-11:

4.2.3.1. Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3. Cyber Systems, associated with communication networks and data communication links, between Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4. 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.

4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. Effective Dates: See Implementation Plan for CIP-003-11.

B. Requirements and Measures

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 BCS, 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 BCS (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 BCS (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 BCS, 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 (TCA) and Removable Media malicious code risk mitigation; and

1.2.6. 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.

R2. Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BCS shall implement one or more documented cyber security plan(s) for its low impact BCS, and Shared Cyber Infrastructure (SCI) that supports a low impact BCS, 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 BCS or their BES Cyber Assets (BCA) 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.

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.

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.

C. Compliance

1. **Compliance Monitoring Process**

   1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

   1.2. Evidence Retention: The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

   The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:

   - Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
   - If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
   - The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

   1.3. Compliance Monitoring and Enforcement Program: "Compliance Monitoring and Enforcement Program" or "CMEP" means, depending on the context (1) the NERC Compliance Monitoring and Enforcement Program (Appendix 4C to the NERC Rules of Procedure) or the Commission-approved program of a Regional Entity, as applicable, or (2) the program, department or organization within NERC or a Regional Entity that is responsible for performing compliance monitoring and enforcement activities with respect to Registered Entities' compliance with Reliability Standards.

Violation Severity Levels

R #	Violation Severity Levels (CIP-003-11)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	The Responsible Entity did not address one of the nine topics required by Requirement R1. (Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (Part 1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 by the CIP Senior Manager	The Responsible Entity did not address two of the nine topics required by Requirement R1. (Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (Part 1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but did	The Responsible Entity did not address three of the nine topics required by Requirement R1. (Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (Part 1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did	The Responsible Entity did not address four or more of the nine topics required by Requirement R1. (Part 1.1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1. (Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by Requirement R1 within 18 calendar months of the previous review. (Requirement R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium

R #	Violation Severity Levels (CIP-003-11)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (Part 1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BCS, but did not address one of the seven topics required by Requirement R1. (Part 1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar	complete this approval in less than or equal to 17 calendar months of the previous approval. (Part 1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BCS, but did not address two of the seven topics required by Requirement R1. (Part 1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (Part 1.2) OR	complete this approval in less than or equal to 18 calendar months of the previous approval. (Requirement R1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BCS, but did not address three of the seven topics required by Requirement R1. (Part 1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (Part 1.2) OR	impact BCS as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (Part 1.1) OR The Responsible Entity did not address four or more of the seven topics required by Requirement R1. (Part 1.2) OR The Responsible Entity did not have any documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1. (Part 1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of

R #	Violation Severity Levels (CIP-003-11)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	months of the previous review. (Part 1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (Part 1.2)	The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (Part 1.2)	The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (Part 1.2)	the previous approval. (Part 1.2)
R2	The Responsible Entity failed to document cyber security awareness according to Requirement R2, Attachment 1, Section 1. (Requirement R2) OR The Responsible Entity failed to document its cyber security plan(s) for	The Responsible Entity failed to reinforce cyber security practices at least once every 15 calendar months according to Requirement R2, Attachment 1, Section 1. (Requirement R2) OR The Responsible Entity failed to document physical security	The Responsible Entity failed to implement the physical security controls according to Requirement R2, Attachment 1, Section 2. (Requirement R2) OR The Responsible Entity failed to permit only necessary inbound and outbound electronic access controls	The Responsible Entity failed to document and implement one or more cyber security plan(s) according to Requirement R2, Attachment 1. (Requirement R2)

R #	Violation Severity Levels (CIP-003-11)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	electronic access controls according to Requirement R2, Attachment 1, Section 3. (Requirement R2) OR The Responsible Entity failed to document one or more Cyber Security Incident response plan(s) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to update each Cyber Security Incident response plan(s) within 180 days according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to manage its Transient Cyber Asset(s) according to Requirement R2, Attachment 1, Section 5.1. (Requirement R2)	controls according to Requirement R2, Attachment 1, Section 2. (Requirement R2) OR The Responsible Entity failed to document electronic access controls according to Requirement R2, Attachment 1, Section 3. (Requirement R2) OR The Responsible Entity failed to implement authentication for all Dial-up Connectivity according to Requirement R2, Attachment 1, Section 3.2 (Requirement R2) OR The Responsible Entity failed to include the process for identification, classification, and response to Cyber Security Incidents according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to document the	according to Requirement R2, Attachment 1, Section 3.1. (Requirement R2) OR The Responsible Entity failed to test each Cyber Security Incident response plan(s) at least once every 36 calendar months according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to notify the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible Entity according to Requirement R2,	

R #	Violation Severity Levels (CIP-003-11)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	OR The Responsible Entity failed to document the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2)	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) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to document mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible Entity according to Requirement R2, Attachment 1, Sections 5.1 and 5.3. (Requirement R2) OR The Responsible Entity failed to document mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment	Attachment 1, Section 5.1. (Requirement R2) OR The Responsible Entity failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (Requirement R2) OR The Responsible Entity failed to implement mitigation for the threat of detected malicious code on the Removable Media prior to connecting Removable Media according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2)	

R #	Violation Severity Levels (CIP-003-11)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		1, Section 5.2. (Requirement R2) OR The Responsible Entity failed to implement the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2)		
R3	The Responsible Entity did not document changes to the CIP Senior Manager within 30 calendar days but did document this change in less than 40 calendar days of the change. (Requirement R3)	The Responsible Entity did not document changes to the CIP Senior Manager within 40 calendar days but did document this change in less than 50 calendar days of the change. (Requirement R3)	The Responsible Entity did not document changes to the CIP Senior Manager within 50 calendar days but did document this change in less than 60 calendar days of the change. (Requirement R3)	The Responsible Entity did not identify, by name, a CIP Senior Manager. OR The Responsible Entity did not document changes to the CIP Senior Manager within 60 calendar days of the change. (Requirement R3)
R4	The Responsible Entity did not document changes to the delegate within 30 calendar days but did document this change in less than 40 calendar days of the change. (Requirement R4)	The Responsible Entity did not document changes to the delegate within 40 calendar days but did document this change in less than 50 calendar days of the change. (Requirement R4)	The Responsible Entity did not document changes to the delegate within 50 calendar days but did document this change in less than 60 calendar days of the change. (Requirement R4)	The Responsible Entity does not have a process to delegate actions from the CIP Senior Manager. (Requirement R4) OR The Responsible Entity did not document changes to the

R #	Violation Severity Levels (CIP-003-11)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				delegate within 60 calendar days of the change. (Requirement R4)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

- Implementation Plan for Project 2023-04
- CIP-003-11 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-003-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
6	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient

Version	Date	Action	Change Tracking
			devices and low impact BES Cyber Systems.
6	1/21/16	FERC Order issued approving CIP-003-6. Docket No. RM15-14-000	
7	2/9/17	Adopted by the NERC Board of Trustees.	Revised to address FERC Order No. 822 directives regarding (1) the definition of LERC and (2) transient devices.
7	4/19/18	FERC Order issued approving CIP-003-7. Docket No. RM17-11-000	
8	5/9/19	Adopted by the NERC Board of Trustees.	Removed SPS references. Revised to address FERC Order No. 843 regarding mitigating the risk of malicious code.
8	7/31/2019	FERC Order issued approving CIP-003-8. Docket No. RD19-5-000.	
9	11/16/2022	Adopted by the NERC Board of Trustees.	Revisions to address NERC Board Resolution and the Supply Chain Report
9	3/16/2023	FERC Order issued approving CIP-003-9. Docket No. RD23-3-000.	
10	5/9/2024	Adopted by the NERC Board of Trustees.	Modifications made by Project 2016-02
11	12/10/2024	Adopted by the NERC Board of Trustees	Modifications made by Project 2023-04

Attachment 1

Required Sections for Cyber Security Plan(s)

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 BCS ratings can utilize policies, procedures, and processes for their high or medium impact BCS including any supporting SCI 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 BCS within the asset, and (2) the Cyber Asset(s) or Virtual Cyber Asset (VCA), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1.1, if any.

Section 3. Electronic Access Controls: Each Responsible Entity shall control electronic access as outlined below.

3.1 For each asset containing low impact BCS identified pursuant to CIP-002 and for SCI that supports a low impact BCS, if any, where electronic access is:

i. Between:
- a low impact BCS; or
- an SCI that supports a low impact BCS

and a Cyber System(s) outside the asset containing:
- the low impact BCS(s); or
- the SCI that supports a low impact BCS;

ii. using a routable protocol when entering or leaving the asset containing the low impact BCS or SCI that supports a low impact BCS; and

iii. not used for time-sensitive communications of Protection Systems;

the Responsible Entity shall implement one or more controls, where Section 3.1. Parts (i), (ii), and (iii) are met, that:

3.1.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity;

3.1.2 Detect known or suspected malicious communications for

both inbound and outbound electronic access;

3.1.3 Authenticate each user prior to permitting access to a network(s) containing low impact BCS or SCI that supports a low impact BCS, through which user-initiated electronic access applicable to Section 3.1 is subsequently permitted;

3.1.4 Protect user authentication information for user-initiated electronic access applicable to Section 3.1.3 while in transit between the Cyber System(s) outside the asset containing low impact BCS or SCI that supports a low impact BCS and

- the authentication system used to meet Section 3.1.3, or
- the asset containing low impact BCS or SCI that supports a low impact BCS;

3.1.5 Include one or more method(s) for determining vendor electronic access, where vendor electronic access is permitted; and

3.1.6 Include one or more method(s) for disabling vendor electronic access, where vendor electronic access is permitted.

3.2 For each asset containing low impact BCS identified pursuant to CIP-002 and for SCI that supports a low impact BCS, if any, the Responsible Entity shall implement one or more control(s) that authenticate all Dial-up Connectivity, if any, that provides access to low impact BCS or SCI that supports a low impact BCS, per system 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. TCA 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 BCS, through the use of TCA or Removable Media. The plan(s) shall include:

5.1 For TCA 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 TCA 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 TCA 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 (per TCA capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review of system hardening used by the party; or
- Review of other method(s) to mitigate the risk of 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 TCA.

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 or VCA other than a BCS or SCI that supports a low impact BCS; 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 BCS or SCI that supports a low impact BCS.

Attachment 2

Examples of Evidence for Cyber Security Plan(s)

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:
  a. The asset, if any, or the locations of the low impact BCS within the asset; and
  b. The Cyber System(s) specified by the Responsible Entity that provide(s) electronic access controls implemented for Attachment 1, Section 3.1.1, if any.

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

1. For Section 3.1.1, documentation showing the permittance of only inbound and outbound electronic access, where electronic access meets Section 3.1, Parts (i), (ii), and (iii), that the Responsible Entity deems necessary, such as:
   - Representative diagrams that illustrate control of inbound and outbound communication(s) between the low impact BCS or SCI that supports a low impact BCS and a Cyber System outside the asset containing low impact BCS.
   - Lists of implemented electronic access controls (e.g., access control lists restricting IP addresses, ports, or services; implementing unidirectional gateways); or
   - Original equipment manufacturer (OEM) specification sheets that provide rationale around necessary electronic access.

2. For Section 3.1.2, documentation showing the ability to detect known or suspected malicious communications for both inbound and outbound electronic access, where electronic access meets Section 3.1, Parts (i), (ii), and (iii), such as:
    - Anti-malware technologies;
    - Intrusion detection system (IDS)/intrusion prevention system (IPS);
    - Monitor or alert for changes to communication baselines;
    - Logging and alerting configuration for security incident and event management (SIEM) systems or other event correlation systems;
    - Automated or manual log reviews;
    - Alerting; or
    - Other operational, procedural, or technical controls.
3. For Section 3.1.3, documentation showing the ability to authenticate each user prior to permitting access to a network(s) containing low impact BCS or SCI that supports a low impact BCS through which user-initiated electronic access applicable to Section 3.1 is subsequently permitted, such as:
    - Authentication mechanism(s) including, but not limited to:
        - Utilization of public key infrastructure (PKI), lightweight directory access protocol (LDAP), remote authentication dial-in user service (RADIUS), and/or similar implemented solutions; or
        - Enforcement of multi-factor authentication (MFA).
    - Virtual private network (VPN) configuration(s) with logs demonstrating enforcement of username and password parameters;
    - Terminal server, jump server, access control device, or an Intermediate System also used with a High or Medium Impact BCS; or
    - Other operational, procedural, or technical controls.
4. For Section 3.1.4, documentation showing the ability to protect user authentication information for user-initiated electronic access applicable to Section 3.1.3 while in transit between the Cyber System outside the asset containing low impact BCS or SCI that supports a low impact BCS and
    - The authentication system used to meet Section 3.1.3, or
    - The asset containing low impact BCS or SCI that supports a low impact BCS,

    such as protection mechanism(s) including, but not limited to:
    - Implementation of an encrypted protocol or service (hypertext transfer protocol secure (HTTPS), secure shell (SSH), etc.);
    - Implementation of an IPsec or secure sockets layer (SSL) VPN; or

- Other operational, procedural, or technical controls.

5. For Section 3.1.5 documentation showing one or more methods for determining vendor electronic access, where vendor electronic access is permitted and electronic access meets Section 3.1, Parts (i), (ii), and (iii), such as:
   - 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.
6. For Section 3.1.6, documentation showing one or more methods for disabling vendor electronic access, where vendor electronic access is permitted and electronic access meets Section 3.1, Parts (i), (ii), and (iii), such as:
   - Disabling vendor electronic 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 access;
   - Disabling communications protocols (such as IP) used for systems which establish and/or maintain vendor electronic 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 access; or
   - Other operational, procedural, or technical controls.
7. For Section 3.2, 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 BCS).

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. TCA 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 TCA 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 TCA 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 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 TCA managed by a party other than the Responsible Entity. If a TCA 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 TCA 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 TCA 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.