A. Introduction

1. **Title:** Cyber Security — BES Cyber System Logical Isolation

2. **Number:** CIP-005-7

3. **Purpose:** To protect BES Cyber System(s) against compromise by permitting only known and controlled communication to and from the system and logically isolating all other communication.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements in this standard , 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

DRAFT

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements in this standard, 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-005-6:

4.2.3.1. Cyber Assets or Virtual Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets or Virtual Cyber Assets associated with communication links logically isolated from, but not providing logical isolation for, BES Cyber Systems or SCI.

DRAFT

4.2.3.3. Cyber Assets or Virtual Cyber Assets associated with communication links between Cyber Assets or Virtual Cyber Assets performing logical isolation 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.

4.2.3.6. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Effective Date:

See Implementation Plan for Project 2016-02 (CIP-005-7).

6. Background: Standard CIP-005 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

DRAFT

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicability Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002 identification and categorization processes.
- **High Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to high impact BES Cyber Systems with Dial-up Connectivity.
- **High Impact BES Cyber Systems with External Routable Connectivity** – Only applies to high impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact BES Cyber Systems located at a Control Center.

DRAFT

- **Medium Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to medium impact BES Cyber Systems with Dial-up Connectivity.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

DRAFT

B. Requirements and Measures

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 – Logical Isolation [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 – Logical Isolation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-7 Table R1 – Logical Isolation			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems connected to a network via routable protocol and their associated: • PCA • PACS hosted on SCI • EACMS hosted on SCI Medium Impact BES Cyber Systems connected to a network via routable protocol and their associated: • PCA • PACS hosted on SCI • EACMS hosted on SCI	Permit only needed and controlled communications to and from applicable systems either individually or as a group and logically isolate all other communications, excluding time sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE.	Examples of evidence may include, but is not limited to, documentation that includes the configuration of systems that enforce electronic access control and logical isolation and document business need such as: • Network infrastructure configuration or policies (ACL, VLAN, VXLAN, MPLS, VRF, multi-context, or multi-tenant environment); • SCI configuration or policies (hypervisor, fabric, back-plane, or SAN configuration)

DRAFT

CIP-005-7 Table R1 – Logical Isolation			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	SCI hosting High or Medium Impact BCS or their associated PACS, EACMS, or PCA. Management Modules of SCI hosting High or Medium Impact BCS or their associated PACS, EACMS, or PCA. EACMS that perform logical isolation for a High impact BES Cyber System. EACMS that perform logical isolation for a Medium impact BES Cyber System.	**1.2.1.** Management Systems may only share CPU and memory with other Management Systems and its associated SCI, per system capability. **1.2.2.** Have one or more methods for permitting only needed and controlled communications to and from its Management Interfaces and Management Systems, logically isolating all other communications. **1.2.3.** Deny communications from BES Cyber Systems and their associated PCAs to the Management Interfaces and Management Systems, per system capability.	Examples of evidence may include, but is not limited to, documentation that includes the configuration of systems that enforce access control and logical isolation such as: • Logically isolated out-of-band network infrastructure configuration (ACL, VLAN, VXLAN, MPLS, VRF, multi-context, or multi-tenant environment) • Physically isolated out-of-band network for dedicated Management Interfaces, Management Modules, or Management Systems • SCI configuration or policies showing the isolation of the management plane resources (hypervisor, fabric, back-plane, or SAN configuration)

DRAFT

CIP-005-7 Table R1 – Logical Isolation			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems and their associated: • PCA • PACS hosted on SCI • EACMS hosted on SCI Medium Impact BES Cyber Systems connected to a network via routable protocol and their associated: • PCA • PACS hosted on SCI • EACMS hosted on SCI SCI connected to a network via routable protocol hosting High or Medium Impact BCS or their associated PACS, EACMS, or PCA.	Protect the confidentiality and integrity of the data traversing communication links that span multiple geographical locations, where methods from Part 1.1 and Part 1.2.2 are not applied, excluding Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers subject to CIP-012 and excluding time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).	Evidence may include, but is not limited to, a documents detailing the methods used to protect the confidentiality and integrity of the dat. (e.g., encryption)

DRAFT

CIP-005-7 Table R1 – Logical Isolation			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High Impact BES Cyber Systems with Dial-up Connectivity and their associated: • PCA • PACS hosted on SCI • EACMS hosted on SCI Medium Impact BES Cyber Systems with Dial-up Connectivity and their associated: • PCA • PACS hosted on SCI • EACMS hosted on SCI SCI with dial-up hosting High or Medium Impact BCS or their associated PACS, EACMS, or PCA.	Perform authentication when establishing Dial-up Connectivity with applicable systems, per system capability. .	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.

DRAFT

CIP-005-7 Table R1 – Logical Isolation			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High Impact BES Cyber Systems and their associated: • PCA • PACS hosted on SCI • EACMS hosted on SCI Medium Impact BES Cyber Systems at Control Centers and their associated: • PCA • PACS hosted on SCI • EACMS hosted on SCI SCI at Control Centers hosting High or Medium Impact BCS or their associated PACS, EACMS, or PCA	Have one or more methods for detecting known or suspected malicious Internet Protocol (IP) communications entering or leaving the isolation required by Part 1.1 or Part 1.2.2.	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.

DRAFT

R2. For all remote access that originates from a system not applicable to Requirement Part 1.1 or Part 1.2.2, excluding Dial-up Connectivity and TCAs, the Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts, per system capability, 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.

CIP-005-6 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated PCA. Medium Impact BES Cyber Systems with IRA and their associated PCA. SCI with IRA hosting High or Medium Impact BCS or their associated PACS, EACMS, or PCA. Management Modules with IRA of SCI hosting High or Medium Impact BCS or their associated PACS, EACMS, or PCA.	Ensure that authorized Interactive Remote Access is through an Intermediate System.	Examples of evidence may include, but are not limited to, network diagrams, architecture documents, or Management Systems reports that show all IRA is through an IS.
2.2	Intermediate Systems used to access applicable systems of Part 2.1. Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	Protect the confidentiality and integrity of authorized Interactive Remote Access between the client and the Intermediate System.	An example of evidence may include, but is not limited to, architecture documents detailing where confidentiality and integrity controls initiates and terminates.

DRAFT

CIP-005-6 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	Intermediate Systems used to access applicable systems of Part 2.1. •	Require multi-factor authentication to the Intermediate System.	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.

DRAFT

CIP-005-6 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.4	High Impact BES Cyber Systems and their associated: • PCA • PACS hosted on SCI • EACMS hosted on SCI Medium Impact BES Cyber Systems and their associated: • PCA • PACS hosted on SCI • EACMS hosted on SCI SCI hosting High or Medium Impact BCS or their associated PACS, EACMS, or PCA. Management Modules of SCI hosting High or Medium Impact BCS or their associated PACS, EACMS, or PCA	Have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access).	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.

DRAFT

CIP-005-6 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.5	High Impact BES Cyber Systems and their associated: • PCA • PACS hosted on SCI • EACMS hosted on SCI Medium Impact BES Cyber Systems with and their associated: • PCA • PACS hosted on SCI • EACMS hosted on SCI SCI hosting High or Medium Impact BCS or their associated PACS, EACMS, or PCA. Management Modules of SCI hosting High or Medium Impact BCS or their associated PACS, EACMS, or PCA	Have one or more method(s) to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access).	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).

DRAFT

CIP-005-6 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.6	Intermediate Systems used to access applicable systems of Part 2.1.	**2.6.1.** Intermediate Systems may only share CPU and memory with other Intermediate Systems and its associated SCI. **2.6.2.** Have one or more methods for permitting only needed and controlled communications between Intermediate Systems and applicable systems of Part 2.1.	An example of evidence may include, but is not limited to, documentation that includes the following: • Configuration showing that the CPU and memory can only be shared with other IS. • Configuration showing how communications are controlled between the IS and applicable systems.

DRAFT