The Background, VRF/VSLs, and Guidelines and Technical Basis Sections have been removed for this informal posting. The Project 2016-02 is seeking comments around the concept of the Requirement/Measure language at this time. All other sections will be modified prior to the initial posting.

A. Introduction

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

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

3. **Purpose:** To protect BES Cyber Systems against compromise by allowing only known and controlled communication to and from the system and logically isolating all other communication.

4. **Applicability:**

   4.1. Functional Entities: For 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 explicitly specified.

   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 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 explicitly specified.

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-005-7:

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

4.2.3.2. Cyber Assets associated with communication networks and data communication links between BES Cyber Systems' Logical Isolation Zones.

4.2.3.3. Cyber Assets associated with communication networks and data communication links used to extend a Logical Isolation Zone to more than one geographic location.

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 CIP-005-7.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes to mitigate the risk posed by unauthorized communications to and from applicable systems that collectively include each of the applicable requirement parts in *CIP-005-7 Table R1 – Logical Isolation Zones.* These processes exclude consideration of time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).

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 Zones* and additional Evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-6 Table R1 – Logical Isolation Zones			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Have one or more methods to logically isolate applicable systems, either individually or as a group, by only allowing: 1.1.1. Communication that has documented inbound and outbound access permissions, including the reason for granting access; and 1.2.1. Serial port connectivity such as RS-232 and RS-485. NOTE: The implemented configuration in support of this Part becomes part of the Secure Configuration of the applicable system.	Evidence may include, but is not limited to, configuration of systems that enforce logical isolation such as network infrastructure configuration (ACL, VLAN, VXLAN, MPLS), compute configuration (e.g., Hypervisor, containers), storage system configuration (e.g., SAN, NAS, DAS).

CIP-005-6 Table R1 – Logical Isolation Zones			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated PCS Medium Impact BES Cyber Systems and their associated PCS	Protect the data traversing communication networks used to provide connectivity between components of a Logically Isolated Zone that spans multiple geographic locations to preserve confidentiality and integrity.	Evidence may include, but is not limited to, architecture documents detailing the methods used to mitigate the risk of unauthorized disclosure. Examples include physical protection and the points where encryption initiates and terminates.
1.3	High Impact BES Cyber Systems with Dial-up Connectivity and their associated PCS Medium Impact BES Cyber Systems with Dial-up Connectivity and their associated PCS	Perform authentication when establishing Dial-up Connectivity with applicable Cyber Assets 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.
1.4	High Impact BES Cyber Systems and their associated PCS Medium Impact BES Cyber Systems at Control Centers and their associated PCS	Have one or more methods for detecting known or suspected malicious inbound and outbound communications to and from applicable systems either individually or as grouped in Part 1.1, excluding serial port connectivity such as RS-232 and RS-485.	Evidence may include, but is not limited to, documentation that malicious communications detection methods (e.g. intrusion detection system, application layer firewall, privileged introspection, etc.) are implemented.

R2. Each Responsible Entity shall implement one or more documented processes to mitigate the risk posed by exploitation of Interactive Remote Access that collectively include the applicable requirement parts, per system capability, in *CIP-005-6 Table R2 –Remote Access Management*.

M2. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-6 Table R2 – Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-7 Table R2 Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated PCS Medium Impact BES Cyber Systems and their associated PCS	Have one or more methods to ensure that Interactive Remote Access to applicable systems is through an Intermediate System that is isolated from the BES Cyber System and restricts Interactive Remote Access to only authorized users.	Evidence may include, but is not limited to, network diagrams or architecture documents.
2.2	High Impact BES Cyber Systems and their associated PCS Medium Impact BES Cyber Systems and their associated PCS	Have one or more methods to mitigate the risks posed by unauthorized modification and unauthorized disclosure of data during all Interactive Remote Access sessions that terminate at an Intermediate System.	Evidence may include, but is not limited to, architecture documents detailing the methods used to mitigate the risk of unauthorized disclosure. Examples include illustrating where encryption initiates and terminates.

CIP-005-7 Table R2 Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems and their associate PCS Medium Impact BES Cyber Systems and their associated PCS	Have one or more methods to require multi-factor authentication for all Interactive Remote Access sessions.	Evidence may include, but is not limited to, documents detailing the authentication factors used.

CIP-005-7 Table R2 Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.4	High Impact BES Cyber Systems and their associated PCS Medium Impact BES Cyber Systems and their associated PCS	Have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access).	Evidence may include, but is not limited to documented methods such as: • Methods for accessing logged information or monitoring 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 requiring vendors to call and request a second factor to initiate remote access.

CIP-005-7 Table R2 Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.5	High Impact BES Cyber Systems and their associated PCS Medium Impact BES Cyber Systems and their associated PCS	Have one or more method(s) to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access).	Evidence may include, but is not limited to, documented methods, such as: • Methods to disable vendor remote access for system-to-system remote access; or • Methods to disable vendor Interactive Remote Access at the applicable Intermediate System.

R3. Each Responsible Entity shall implement one or more documented processes to mitigate the risk posed by unrestricted access for communication between the management plane [1] and the data plane[2] that collectively include the applicable requirement parts, in *CIP-005-6 Table R3* – Isolation of Management Plane and Data Plane.

M3. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-6 Table R3* – Isolation of Management Plane and Data Plane and additional evidence to demonstrate implementation as described in the Measures column of the table.

[1] Management plane of a system is that element that configures, monitors, and provides management, monitoring and configuration services to, all layers of the network stack and other parts of the system.

[2] Data plane (sometimes known as the user plane, forwarding plane, carrier plane or bearer plane) is the part of a network that carries user traffic.

CIP-005-6 Table R3 – Isolation of Management Plane and Data Plane			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACS 2. PCS Medium Impact BES Cyber Systems and their associated PCS: 1. EACS 2. PCS	Have one or more methods per system capability to: 1. Restrict access to the management plane; and 2. Logically isolate the management plane from the data plane.	An example of evidence may include but is not limited to documentation that includes the following: Configuration of systems that enforce authentication and logical isolation such as network infrastructure configuration (ACL, VLAN, VXLAN, MPLS), compute configuration (e.g. Hypervisor, containers), storage system configuration (e.g. SAN, NAS, DAS).

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) 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 applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable 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 CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

D. Regional Variances

None.

E. Associated Documents

None.

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 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
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-005-5.	
6	07/20/17	Modified to address certain directives in FERC Order No. 829.	Revised
6	08/10/17	Adopted by the NERC Board of Trustees.	