Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008).
2. SC authorized moving the SAR forward to standard development (July 10, 2008).
3. First posting for 60-day formal comment period and concurrent ballot (November 2011).

Description of Current Draft

This is the second posting of Version 5 of the CIP Cyber Security Standards for a 40-day formal comment period. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. A first posting of Version 5 was posted in November 2011 for a 60-day comment period and first ballot. Version 5 reverts to the original organization of the standards with some changes and addresses the balance of the FERC directives in its Order 706 approving Version 1 of the standards. This posting for formal comment and parallel successive ballot addresses the comments received from the first posting and ballot.

Anticipated Actions	Anticipated Date
40-day Formal Comment Period with Parallel Successive Ballot	April 2012
Recirculation ballot	June 2012
BOT adoption	June 2012

Effective Dates

1. **24 Months Minimum** – The Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval. CIP-003-5, Requirement R2 shall become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[1]
2. In those jurisdictions where no regulatory approval is required, the Version 5 CIP Cyber Security Standards, except for CIP-003-5, Requirement R2, shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, and CIP-003-5, Requirement R2 shall become effective on the first day of the 13th calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

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	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template.	

Definitions of Terms Used in the Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the "Guidelines and Technical Basis" section of the Standard.

A. Introduction

1. **Title:** Cyber Security — Electronic Security Perimeter(s)

2. **Number:** CIP-005-5

3. **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.

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 Facilities described in 4.2.2

   4.1.3 Generator Operator

   4.1.4 Generator Owner

   4.1.5 Interchange Coordinator

   4.1.6 Load-Serving Entity that owns Facilities described in 4.2.1

   4.1.7 Reliability Coordinator

   4.1.8 Transmission Operator

   4.1.9 Transmission Owner

   4.2. Facilities:

   4.2.1 Load Serving Entity: One or more of the UFLS or UVLS Systems that are part of a Load shedding program required by a NERC or Regional Reliability Standard and that perform automatic load shedding under a common control system, without human operator initiation, of 300 MW or more.

   4.2.2 Distribution Provider: One or more of the Systems or programs designed, installed, and operated for the protection or restoration of the BES:

   - A UFLS or UVLS System that is part of a Load shedding program required by a NERC or Regional Reliability Standard and that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more

- A Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is required by a NERC or Regional Reliability Standard
- A Protection System that applies to Transmission where the Protection System is required by a NERC or Regional Reliability Standard
- 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.

4.2.3 Responsible Entities listed in 4.1 other than Distribution Providers and Load-Serving Entities: All BES Facilities.

4.2.4 Exemptions: The following are exempt from Standard CIP-002-5:

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

4.2.4.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.4.3 In nuclear plants, 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.

5. Background:

Standard CIP-005-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

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 a common subject matter.

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. A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

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 they feel necessary in their documented processes, but they 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.
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.

Applicability Columns in Tables:

Each table row has an applicability column to further define the scope to which a specific requirement row applies to BES Cyber Systems and associated Cyber Assets. 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 column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 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.
- **Medium Impact BES Cyber Systems** – Applies to each BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as medium impact according to the CIP-002-5 identification and categorization processes.

- **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.
- **Associated Protected Cyber Assets** – Applies to each Protected Cyber Asset associated with a corresponding high impact BES Cyber System or medium impact BES Cyber System in the applicability column.
- **Electronic Access Points** – Applies at Electronic Access Points associated with a referenced high impact BES Cyber System or medium impact BES Cyber System in the applicability column.

B. Requirements and Measures

Rationale for R1: The Electronic Security Perimeter ("ESP") serves to control traffic at the external electronic boundary of the BES Cyber System. It provides a first layer of defense for network based attacks as it limits reconnaissance of targets, restricts and prohibits traffic to a specified rule set, and assists in containing any successful attacks.

Summary of Changes: CIP-005, Requirement R1 has taken more of a focus on the discrete Electronic Access Points, rather than the logical "perimeter".

CIP-005 (V1 through V4), Requirement R1.2 has been deleted from V5. This requirement was definitional in nature and used to bring dial-up modems using non-routable protocols into the scope of CIP-005. The non-routable protocol exclusion no longer exists as a blanket CIP-002 filter for applicability in V5, therefore there is no need for this requirement.

CIP-005 (V1 through V4), Requirement R1.1 and R1.3 were also definitional in nature and have been deleted from V5 as separate requirements but the concepts were integrated into the definitions of ESP and Electronic Access Point ("EAP").

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-005-5 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 items in *CIP-005-5 Table R1 – Electronic Security Perimeter* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-5 Table R1 – Electronic Security Perimeter			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	All BES Cyber Assets and associated Protected Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.	Evidence may include, but is not limited to, a list of all ESPs with all uniquely identifiable Cyber Assets within each ESP.
Reference to prior version: *CIP-005-4, R1*		**Change Rationale:** E*xplicitly clarifies that BES Cyber Assets connected via routable protocol must be in an Electronic Security Perimeter.*	
1.2	High Impact BES Cyber Systems with External Routable Connectivity Medium Impact BES Cyber Systems with External Routable Connectivity Associated Protected Cyber Assets	All External Routable Connectivity through the ESP must be through an identified Electronic Access Point (EAP).	Evidence may include, but is not limited to, network diagrams showing all external routable communication paths and the identified EAPs.
Reference to prior version: *CIP-005-4, R1*		**Change Rationale:** *Changed to refer to the defined term Electronic Access Point and BES Cyber System.*	

CIP-005-5 Table R1 – Electronic Security Perimeter			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.3	Electronic Access Points for High Impact BES Cyber Systems Electronic Access Points for Medium Impact BES Cyber Systems	Require inbound and outbound access permissions, including the rationale for granting access, and deny all other access by default.	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.
Reference to prior version: *CIP-005-4, R2.1*		**Change Rationale:** *Changed to refer to the defined term Electronic Access Point and to focus on the entity knowing and having a reason for what it allows through the EAP in both inbound and outbound directions.*	
1.4	High Impact BES Cyber Systems with dial-up connectivity Medium Impact BES Cyber Systems with dial-up connectivity	Perform authentication when establishing dial-up connectivity with the BES Cyber System, where technically feasible.	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.
Reference to prior version: *CIP-005-4, R2.3*		**Change Rationale:** *Added clarification that dial-up connectivity should perform authentication so that the BES Cyber System is not directly accessible with a phone number only.*	

CIP-005-5 Table R1 – Electronic Security Perimeter			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
1.5	Electronic Access Points for High Impact BES Cyber Systems Electronic Access Points for Medium Impact BES Cyber Systems at Control Centers	Have a method for detecting malicious communications.	Evidence may include, but is not limited to: 1. Evidence that intrusion detection systems are functioning: • Configuration files of intrusion detection systems deployed to monitor an EAP; or • Logs that were generated by an intrusion detection system; and 2. Documentation showing where intrusion detection systems were deployed.
Reference to prior version: *CIP-005-4, R1*		**Change Rationale:** *Per FERC Order No. 706, Paragraphs 496-503, ESPs need two distinct security measures such that the Cyber Assets do not lose all perimeter protection if one measure fails or is mis-configured. The Order makes clear this is not simple redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.*	

Rationale for R2: Discovery and announcement of vulnerabilities for remote access methods and technologies, that were previously thought secure and in use by a number of electric sector entities, necessitate changes to industry security control standards. Currently, no requirements or guidance documents are available to either require or recommend how secure remote access to BES Cyber Systems can or should be accomplished. Inadequate safeguards for remote access can allow unauthorized access to the organization's network, with potentially serious consequences.

Remote access control procedures must provide adequate safeguards through robust identification, authentication and encryption techniques. Remote access to the organization's network and resources will only be permitted providing that authorized users are authenticated, data is encrypted across the network, and privileges are restricted.

Additional information is provided in ***Guidance for Secure Interactive Remote Access*** published by NERC in July 2011.

Summary of Changes: This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

R2. Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable items, where technically feasible, in *CIP-005-5 Table R2 – Interactive 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 items in *CIP-005-5 Table R2 – Interactive Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-5 Table R2 – Interactive Remote Access Management			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems Associated Protected Cyber Assets	Utilize an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset.	Evidence may include, but is not limited to, network diagrams or architecture documents.
Reference to prior version: *New*		**Change Rationale:** *This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.*	
2.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems Associated Protected Cyber Assets	Utilize encryption for all Interactive Remote Access sessions that terminate at an Intermediate Device in order to protect the confidentiality and integrity of each Interactive Remote Access session.	Evidence may include, but is not limited to, architecture documents detailing where encryption initiates and terminates.
Reference to prior version: *CIP-007-5, R3.1*		**Change Rationale:** *This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.*	

CIP-005-5 Table R2 – Interactive Remote Access Management			
Part	**Applicable BES Cyber Systems and associated Cyber Assets**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems Associated Protected Cyber Assets	Require multi-factor authentication for all Interactive Remote Access sessions. Factors must be at least two of the three following categories: • Something the individual knows (including, but not limited to, passwords or PINs. User ID is not an authentication factor); • Something the individual has (including, but not limited to, tokens, digital certificates, or smart cards); or • Something the individual is (including, but not limited to, fingerprints, iris scans, or other biometric characteristic).	Evidence may include, but is not limited to, architecture documents detailing the authentication factors used.
Reference to prior version: *CIP-007-5, R3.2*		**Change Rationale:** *This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The multi-factor authentication methods are also the same as those identified in the Homeland Security Presidential Directive 12 (HSPD-12), issued August 12, 2007.*	

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional entity approved by FERC or other applicable governmental authority shall serve as the CEA.

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.

- Each Responsible Entity shall retain data or evidence for each requirement in this standard for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.
- 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 duration 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 Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning and Same Day Operations**	**Medium**	The Responsible Entity failed to document one or more processes for *CIP-005-5 Table R1 – Electronic Security Perimeter* according to Requirement R1. OR The Responsible Entity failed to document 5% or less of External Routable Connectivity through the ESP through an identified Electronic Access Point (EAP) according to Requirement R1, part 1.2; OR The Responsible Entity failed to document 5% or less of inbound and outbound access permissions, including	The Responsible Entity failed to document more than 5% but less than or equal to 10% of External Routable Connectivity through the ESP through an identified Electronic Access Point (EAP) according to Requirement R1, part 1.2; OR The Responsible Entity failed to document more than 5% but less than or equal to 10% of inbound and outbound access permissions, including the rationale for granting access according to Requirement R1, part 1.3.	The Responsible Entity failed to document more than 10% but less than or equal to 15% of External Routable Connectivity through the ESP through an identified Electronic Access Point (EAP) according to Requirement R1, part 1.2; OR The Responsible Entity failed to document more than 10% but less than or equal to 15% of inbound and outbound access permissions, including the rationale for granting access according to Requirement R1, part 1.3.	The Responsible Entity failed to document more than 15% of External Routable Connectivity through the ESP through an identified Electronic Access Point (EAP) according to Requirement R1, part 1.2; OR The Responsible Entity failed to document more than 15% of inbound and outbound access permissions, including the rationale for granting access according to Requirement R1, part 1.3. OR The Responsible Entity

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			the rationale for granting access according to Requirement R1, part 1.3.			did not have all BES Cyber Assets and associated Protected Cyber Assets connected to a network via a routable protocol within a defined ESP according to Requirement R1, part 1.1. OR External Routable Connectivity through the ESP was not through an identified EAP according to Requirement R1, part 1.2. OR The Responsible Entity did not require inbound and outbound access permissions and deny all other access by default according to

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						Requirement R1, part 1.3. OR The Responsible Entity did not perform authentication when establishing dial-up connectivity with the BES Cyber System, where technically feasible according to Requirement R1, part 1.4. OR The Responsible Entity did not have a method for detecting malicious communications according to Requirement R1, part 1.5.
R2	**Operations Planning and Same Day Operations**	**Medium**	The Responsible Entity failed to document one or more processes for *CIP-005-5 Table R2 – Interactive Remote*	The Responsible Entity failed to implement the required multi-factor authentication according to	The Responsible Entity failed to implement one of the following: • Intermediate	The Responsible Entity failed to implement two or more of the following:

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Access according to Requirement R2.	Requirement R2, Part 2.3.	Device according to Requirement R2, Part 2.1; OR • Encryption according to Requirement R2, Part 2.2.	• Intermediate Device according to Requirement R2, Part 2.1 (2.1); • Encryption according to Requirement R2, Part 2.2; OR • Multi-factor authentication according to Requirement R2, Part 2.3.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Requirement R1:

CIP-005-5, Requirement R1 requires segmenting of BES Cyber Systems from other systems of differing trust levels by requiring controlled Electronic Access Points between the different trust zones. Electronic Security Perimeters are also used as a primary defense layer for some BES Cyber Systems that may not inherently have sufficient cyber security functionality, such as devices that lack authentication capability.

All BES Cyber Systems that are connected to a network via a routable protocol must have a defined Electronic Security Perimeter (ESP). Even standalone networks that have no external connectivity to other networks must have a defined ESP. The ESP defines a zone of protection around the BES Cyber System, and it also provides clarity for entities to determine what systems or Cyber Assets are in scope and what requirements they must meet. The ESP is used in:

- Defining the scope of 'Associated Protected Cyber Assets' that must also meet certain CIP requirements.
- Defining the boundary in which all of the Cyber Assets must meet the requirements of the highest impact BES Cyber System that is in the zone (the 'high water mark').

The standard does not require segmenting of BES Cyber Systems by impact classification, and many different impact classifications can be mixed within an ESP. However, all of the Cyber Assets and systems within the ESP will be elevated to the level of the highest impact BES Cyber System present in the ESP. The standard handles this by defining all other Cyber Assets within the ESP, even other BES Cyber Systems of lesser impact, as "Protected Cyber Assets" of the highest impact system in the ESP.

For example, if an ESP contains both a high impact BES Cyber System and a low impact BES Cyber System, the each Cyber Asset of the low impact BES Cyber System is an "Associated Protected Cyber Asset" of the high impact BES Cyber System and must meet all requirements with that designation in the applicability columns of the requirement tables.

If there is routable connectivity across the ESP into any Cyber Asset, then an Electronic Access Point (EAP) must control traffic into and out of the ESP. Responsible Entities should know what traffic needs to cross an EAP and document those reasons to ensure the EAPs limit the traffic to only those known communication needs. These include, but are not limited to, communications needed for normal operations, emergency operations, support, maintenance, and troubleshooting.

The EAP should control both inbound and outbound traffic. The standard added outbound traffic control, as it is a prime indicator of compromise. If Cyber Assets within the ESP become compromised and attempt to communicate to unknown hosts outside the ESP (usually 'command and control' hosts on the Internet, or compromised 'jump hosts' within the Responsible Entity's other networks acting as intermediaries), the EAPs should function as a first level of defense in stopping the exploit. This does not limit the Responsible Entity from controlling outbound traffic at the level of granularity that it deems appropriate, and large

ranges of internal addresses may be allowed. The SDT's intent is that the Responsible Entity knows what other Cyber Assets or ranges of addresses a BES Cyber System needs to communicate with and limits the communications to that known range. For example, most BES Cyber Systems within a Responsible Entity should not have the ability to communicate through an EAP to any network address in the world, but should probably be at least limited to the address space of the Responsible Entity, and preferably to individual subnet ranges or individual hosts within the Responsible Entity's address space. The SDT's intent is not for Responsible Entities to document the inner workings of stateful firewalls, where connections initiated in one direction are allowed a return path. The intent is to know and document what systems can talk to what other systems or ranges of systems on the other side of the EAP, such that rogue connections can be detected and blocked.

This requirement applies only to communications for which access lists and 'deny by default' type requirements can be universally applied, which today are those that employ routable protocols. Direct serial, non-routable, connections are not included as there is no perimeter or firewall type security that should be universally mandated across all entities and all serial communication situations. There is no firewall or perimeter capability for an RS232 cable run between two Cyber Assets. Without a clear 'perimeter type' security control that can be applied in practically every circumstance, such a requirement would mostly generate technical feasibility exceptions ("TFEs") rather than increased security.

As for dial-up connectivity, the SDT's intent of this requirement is to prevent situations where only a phone number can establish direct connectivity to the BES Cyber Asset. If a dial-up modem is implemented in such a way that it simply answers the phone and connects the line to the BES Cyber Asset with no authentication of the calling party, it is a vulnerability to the BES Cyber System. The requirement calls for some form of authentication of the calling party before completing the connection to the BES Cyber System. Some examples of acceptable methods include dial-back modems, modems that must be remotely enabled or powered up, and modems that are only powered on by onsite personnel when needed along with policy that states they are disabled after use. If the dial-up connectivity is used for Interactive Remote Access, then the Requirement R2 requirements also apply.

The standard adds a requirement to detect malicious communications for Control Centers. This is in response to FERC Order No. 706, Paragraphs 496-503, where ESPs are required to have two distinct security measures such that the BES Cyber Systems do not lose all perimeter protection if one measure fails or is mis-configured. The Order makes clear that this is not simple redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs. Technologies meeting this requirement include Intrusion Detection or Intrusion Prevention Systems (IDS/IPS) or other forms of deep packet inspection. These technologies go beyond source/destination/port rule sets and thus provide another distinct security measure at the ESP.

Requirement R2:

See Secure Remote Access Reference Document (see remote access alert).